MITNICK

A ARTE DE ENGANAR

Kevin D. Mitnick & William L. Simon

Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação

MAKRON
Books

PEARSON
Education

Prefácio de Steve Wozniak

As aventuras de Kevin Mitnick como cibercriminoso e fugitivo de uma das caçadas mais exaustivas da história do FBI deram origem a dezenas de artigos, livros, filmes e documentários. Desde que foi solto de uma prisão federal, Mitnick deu uma virada *na* sua vida e estabeleceu-se como um dos especialistas em segurança de computadores mais requisitados de todo o mundo.

Neste livro, o hacker mais famoso do mundo fornece orientações específicas para o desenvolvimento de protocolos, programas de treinamento e manuais para garantir que o investimento em segurança técnica sofisticada de uma empresa não seja em vão. Ele dá conselhos sobre como evitar vulnerabilidades de segurança e espera que as pessoas estejam sempre preparadas para um ataque vindo do risco mais sério de todos — a natureza humana.

MITNICK

A ARTE DE ENGANAR

Kevin D. Mitnick & William L. Simon

Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação

Tradução:
Kátia Aparecida Roque

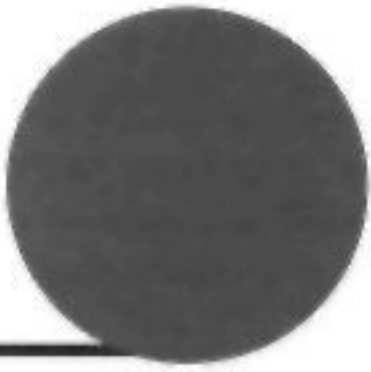
Revisão Técnica:
Olavo José Anchieschi Gomes
Coordenador de projetos de segurança em informações. Especialista em segurança de redes e ethical hacking. Atua no desenvolvimento de políticas de segurança e análise de vulnerabilidades em redes LAN/WAN.

PEARSON
Education

São Paulo

Brasil Argentina Colômbia Costa Rica Chile Espanha
Guatemala México Peru Porto Rico Venezuela

Para Shelly Jaffe, Reba Vartanian, Chickie Leventhal e Mitchell Mitnick
e para os falecidos Alan Mitnick, Adam Mitnick
e Jack Biello

Para Arynne, Victoria e David, Sheldon,
Vincent e Elena

Engenharia social

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Sumário

Apresentação

Nós nascemos com um impulso interno de explorar a natureza daquilo que nos cerca. Como todos os jovens, Kevin Mitnick e eu éramos muito curiosos sobre o mundo e ansiosos para testar a nós mesmos. Quase sempre fomos recompensados pelas nossas tentativas de aprender coisas novas, solucionar quebra-cabeças e ganhar jogos. Mas ao mesmo tempo, o mundo ao nosso redor nos ensinou regras de comportamento que restringiam nossa necessidade de exploração livre. Para os nossos ousados cientistas e empreendedores tecnológicos, bem como para pessoas como Kevin Mitnick, seguir essa vontade traz as maiores emoções e permite que realizemos coisas que os outros acreditam que não podem ser feitas.

Kevin Mitnick é uma das melhores pessoas que conheço. Pergunte e ele responderá de forma direta que aquilo que ele fazia — a engenharia social — era trapacear as pessoas. Mas Kevin não é mais um engenheiro social. E mesmo quando o era, o seu motivo nunca foi enriquecer ou causar danos às outras pessoas. Isso não quer dizer que não existam criminosos perigosos e destrutivos que usam a engenharia social para causar danos reais. Na verdade, foi exatamente por esse motivo que Kevin escreveu este livro — para avisá-los sobre eles.

Este livro mostra como somos vulneráveis — o governo, as empresas e cada um de nós — às invasões do engenheiro social. Nessa era de conscientização sobre a segurança, gastamos somas imensas em tecnologia para proteger nossas redes de computadores e nossos dados. Este livro mostra como é fácil enganar quem trabalha nessas áreas e burlar toda essa proteção tecnológica.

Trabalhando em empresas ou no governo, forneço aqui um mapa para ajudá-lo a entender como os engenheiros sociais trabalham e o que você pode fazer para frustrá-los. Usando histórias fictícias que são divertidas e elucidativas, Kevin e Bill Simon dão vida a técnicas do submundo da engenharia social. Após cada uma das histórias, há orientações práticas que o ajudam a se proteger contra as invasões e ameaças descritas.

A segurança tecnológica deixa grandes lacunas que pessoas como Kevin podem nos ajudar a fechar. Leia este livro e você finalmente perceberá que todos nós precisamos recorrer aos Mitnicks que há entre nós para obter orientação.

— **Steve Wozniak**

Prefácio

Alguns hackers destroem os arquivos ou unidades de disco inteiras das pessoas. Eles são chamados de *Crackers* ou *vândalos.* Alguns hackers novatos não se preocupam em aprender a tecnologia; eles apenas querem baixar as ferramentas dos hackers para entrar nos sistemas de computadores, Esses são chamados de *script kiddies.* Os hackers mais experientes, com habilidades em programação, desenvolvem programas para hackers e os postam na Web e nos sistemas de bulletin board. Em seguida, temos os indivíduos que não têm nenhum interesse em tecnologia, mas que usam o computador apenas como uma ferramenta que os ajuda a roubar dinheiro, bens ou serviços.

Apesar do mito que a mídia criou sobre Kevin Mitnick, não sou um hacker malicioso.

Mas estou me adiantando na história.

O INÍCIO

O meu caminho provavelmente foi definido no início da minha vida. Eu era uma criança bonita e feliz, mas chateada. Após meu pai sair de casa quando eu tinha três anos, a minha mãe trabalhou como garçonete para nos sustentar Naquela época — apenas uma criança criada por uma mãe que trabalhava muito, sem um horário fixo — eu era um jovem que me cuidava por conta própria quase que de manhã até a noite. Eu era a minha própria babá.

Cresci em uma comunidade do Vale de São Fernando e tinha toda a Los Angeles para explorar; com doze anos já havia descoberto um meio de viajar de graça em toda a área da Grande Los Angeles. Percebi certo dia que o bilhete de baldeação de ônibus que havia comprado baseava-se em um padrão incomum de furos em papel que os motoristas usavam para marcar o dia, a hora e o itinerário nos bilhetes. Um motorista amigo, ao responder minhas perguntas cuidadosamente formuladas, contou-me onde eu poderia comprar aquele tipo especial de furador de papel.

As baldeações permitem que você troque de ônibus e continue a viagem até o seu destino, mas eu havia descoberto como usá-las para viajar para qualquer lugar que quisesse de graça. A obtenção das passagens em branco foi como passear no parque: as lixeiras dos terminais de ônibus estavam cheias de blocos de passagens parcialmente usados, os quais eram jogados pelos motoristas no final de seus turnos. Com um bloco de passagens em branco e o furador, podia marcar minhas próprias baldeações e viajar para qualquer parte aonde fossem os ônibus de Los Angeles. Em pouco tempo, já tinha feito tudo, menos decorar os horários dos ônibus de todo o sistema. Esse foi um exemplo precoce da minha surpreendente memória para determinados tipos de informações; ainda hoje consigo decorar números de telefone, senhas e outras coisas.

Outro interesse pessoal que surgiu logo cedo foi o meu fascínio pela mágica. Após aprender como um truque novo funcionava, não parava de praticar até dominá-lo bem. De certa forma, foi pela mágica que descobri como é bom enganar as pessoas.

Do phreaking ao hacking

O meu primeiro encontro com aquilo que aprenderia a chamar de *engenharia social* deu-se durante meus anos no ginásio, quando conheci outro aluno que foi pego com um hobby chamado *phone phreaking.* Esse é um tipo de hacking que permite que você vasculhe a rede telefônica explorando os sistemas de telefone e os empregados da empresa de telefonia. Ele me mostrou os truques que podia fazer com um telefone, como conseguir todas as informações que a empresa de telefonia tinha sobre um cliente e como usar um número de teste secreto para fazer ligações interurbanas de graça (na verdade elas eram de graça para nós — descobri bem mais tarde que aquele não era um número secreto de teste: as ligações eram cobradas de alguma conta MCI da pobre empresa).

Essa foi a minha apresentação à engenharia social — o meu jardim da infância, por assim dizer. Ele garoto e outro phreaker que conheci pouco tempo depois me deixavam escutar as ligações de *pretexto* para a empresa de telefonia. Eu ouvia as coisas que eles diziam para parecerem pessoas de credibilidade, aprendi sobre os diferentes escritórios das empresas de telefonia, o linguajar e os procedimentos. Mas esse "treinamento" não durou muito tempo; ele não precisava ser longo. Em breve estava aprendendo por conta própria e me saindo melhor ainda do que aqueles primeiros professores.

O curso que a minha vida tomaria nos próximos 15 anos já estava definido.

Uma das minhas peças preferidas era conseguir o acesso não autorizado a uma central telefônica e mudar a classe de serviços de um colega phreaker. Quando tentava fazer uma ligação de casa, ele ouvia uma mensagem pedindo para depositar vinte e cinco centavos, porque a central da empresa de telefonia havia recebido informações de que ele estava ligando de um telefone público.

Fiquei interessado em tudo que dissesse respeito a telefones — não apenas a eletrônica, às centrais e aos computadores, mas também a organização corporativa, aos procedimentos e a terminologia. Após algum tempo, talvez já soubesse mais sobre o sistema de telefones do que qualquer empregado da empresa. E havia desenvolvido as minhas habilidades em engenharia social até o ponto de com 17 anos poder falar com a maioria dos empregados da empresa de telefonia sobre quase tudo, fosse pessoalmente ou por telefone.

A minha carreira tão divulgada de hacker, na verdade, começou quando eu estava no colégio. Embora não possa descrever aqui os detalhes, basta dizer que um dos principais incentivos para as minhas primeiras ações foi ser aceito pelos caras do grupo de hackers.

Naquela época usávamos o termo *hacker* para descrever uma pessoa que passava grande parte do tempo mexendo com hardware e software, seja para o desenvolvimento de programas mais eficientes, seja para eliminar etapas desnecessárias e fazer um trabalho mais rapidamente. O termo agora se tornou pejorativo com o significado de "criminoso malicioso". Uso o termo como sempre o usei --- no seu sentido mais antigo e benigno.

Terminado o colégio, fiz um curso sobre computadores no Computer Learning Center, em Los Angeles. Em alguns meses, o gerente de computadores da escola percebeu que eu havia descoberto uma vulnerabilidade no sistema operacional e havia ganhado privilégios administrativos totais sobre seu minicomputador IBM. Os melhores especialistas em computadores do seu corpo docente não conseguiram descobrir como eu havia feito aquilo. Este deve ter sido um dos primeiros exemplos de "contrate o hacker", pois recebi uma oferta irrecusável: criar um projeto *honors* (dentro dos padrões e

normas) para melhorar a segurança dos computadores da escola, ou enfrentar a suspensão por ter invadido o sistema. É claro que preferi criar o projeto e acabei me formando *Cum Laude with Honors,*

Tomando-me um engenheiro social

Algumas pessoas acordam de manhã temendo a sua rotina de trabalho nas proverbiais minas de sal. Tive sorte e gosto do meu trabalho. Você não pode imaginar o desafio, a gratificação e o prazer que sentia no período em que trabalhei como detetive particular. Eu estava aperfeiçoando meus talentos na arte teatral chamada *engenharia social* — fazer com que as pessoas façam coisas que normalmente não fariam para um estranho — e sendo pago para fazer isso.

Para mim não foi difícil tornar-me proficiente em engenharia social. O lado paterno da minha família trabalhava com vendas há gerações, de modo que a arte da influência e persuasão pode ter sido um traço que herdei. Quando você combina uma inclinação para enganar as pessoas com os talentos da influência e persuasão, você chega ao perfil de um engenheiro social

Pode-se dizer que há duas especialidades dentro da classificação do cargo de artista da trapaça. Alguém que faz falcatruas e engana as pessoas para tirar o seu dinheiro pertence a uma subespecialidade chamada *grifter*. Alguém que usa a fraude, a influência e a persuasão contra as empresas, em geral visando suas informações, pertence a outra subespecialidade: o *engenheiro social.* Desde a época do meu truque com a baldeação de ônibus, quando era jovem demais para saber que era errado aquilo que estava fazendo, eu havia começado a reconhecer um talento para descobrir os segredos que eu não deveria saber, Aproveitei aquele talento usando a fraude, conhecendo o jargão e desenvolvendo uma habilidade de manipulação bem lapidada.

Uma forma que descobri para desenvolver as habilidades da minha arte, se é que posso chamá-la de arte, foi escolher algumas informações com as quais não me importava e ver se poderia convencer alguém do outro lado do telefone a me fornecê-las, só para melhorar as minhas habilidades. Da mesma forma que costumava praticar meus truques de mágica, pratiquei a criação de pretextos. Por meio de todos esses ensaios, logo descobri que poderia adquirir praticamente quaisquer informações que desejasse.

Como descrevi em meu testemunho no Congresso perante os Senadores Lieberman e Thompson anos depois:

> *Tive acesso não autorizado aos sistemas de computadores de algumas das maiores corporações do planeta, e consegui entrar com sucesso em alguns dos sistemas de computadores mais protegidos que já foram desenvolvidos. Usei meios técnicos e não técnicos para obter o código-fonte de diversos sistemas operacionais e dispositivos de telecomunicações para estudar suas vulnerabilidades e seu funcionamento interno.*

Toda essa atividade visava satisfazer minha própria curiosidade, ver o que eu poderia fazer e descobrir informações secretas sobre os sistemas operacionais, telefones celulares e tudo o que chamasse minha atenção.

ÚLTIMAS IDÉIAS

Reconheci desde a minha prisão que minhas ações eram ilegais e que cometi invasões de privacidade.

Meus crimes foram motivados pela curiosidade. Eu queria saber o máximo possível sobre o modo como funcionavam as redes de telefonia e os prós e Contras da segurança de computadores.

Passei de uma criança que adorava fazer truques de mágica para o hacker mais conhecido do mundo, temido pelas corporações e pelo governo. Ao pensar nesses últimos 30 anos, tenho de admitir que tomei algumas decisões ruins, motivadas pela minha curiosidade, pelo desejo de aprender sobre a tecnologia e pela necessidade de um bom desafio intelectual.

Hoje sou outra pessoa. Estou transformando meus talentos e o extenso conhecimento que reuni sobre a segurança das informações e sobre as táticas da engenharia social para ajudar o governo, as empresas e os indivíduos a evitar, detectar e responder às ameaças da segurança da informação.

Este livro é mais uma forma pela qual posso usar a minha experiência para ajudar os outros a evitarem os esforços dos ladrões mal-intencionados de informações de todo o mundo. Creio que o leitor achará as histórias agradáveis, elucidativas e educativas.

Introdução

Este livro contém inúmeras informações sobre a segurança das informações e a engenharia social. Para ajudá-lo a encontrar o seu caminho, apresento a sua organização:

Na Parte 1, revelo o elo mais fraco da segurança e mostro o motivo pelo qual você e a sua empresa estão arriscados a sofrer ataques da engenharia social

Na Parte 2, você verá como os engenheiros sociais brincam com a sua confiança, com o seu desejo de ser útil, com a sua simpatia e com a sua credulidade para obter aquilo que eles querem. As histórias fictícias de ataques típicos demonstrarão que os engenheiros sociais podem assumir muitos
Se acha que nunca encontrou um, provavelmente está errado. Você reconheceria um cenário no qual já esteve nessas histórias e se perguntaria seja teve um contato com a engenharia social? Isso é bem possível. Mas depois de ler os Capítulos 2 a 9, você saberá como ter a palavra final quando o próximo engenheiro social ligar.

Na Parte 3, você vê como o engenheiro social faz as suas apostas em histórias criadas para mos¬trar como ele pode entrar nas instalações da sua corporação, roubar o tipo de segredo que pode criar ou destruir a sua empresa e frustrar as suas medidas de segurança de alta tecnologia. Os cenários desta seção o conscientizarão sobre as ameaças que variam da simples vingança de um empregado ate o ciberterrorismo. Se você valoriza as informações que mantêm a sua empresa funcionando e a privacidade dos seus dados, vai querer ler os Capítulos 10 a 14 do início ao final.

É importante observar que a menos que seja declarado o contrário, as piadas deste livro são puramente fictícias.

Na Parte 4, falo em linguagem corporativa sobre como evitar ataques bem-sucedidos da engenharia social na sua organização. O Capítulo 15 fornece um roteiro de um programa de treinamento em segurança bem-sucedido. E o Capítulo 16 pode salvar o seu pescoço — ele traz uma política de segurança completa que você pode personalizar para a sua organização e implementar imediatamente para manter seguras a sua empresa e as suas informações.

Finalmente, forneci uma seção Segurança Rápida, que inclui listas de verificação, tabelas e gráficos que resumem as principais informações que você pode usar para ajudar seus empregados a frustrar um ataque da engenharia social no trabalho. Essas ferramentas também fornecem informações valiosas que você pode usar para criar seu próprio programa de treinamento em segurança.

Você também encontra diversos elementos úteis: as caixas de texto "Jargão" fornecem as definições da engenharia social e a terminologia dos hackers de computadores, os "Recados do Mitnick" oferecem em poucas palavras o conhecimento para ajudar a fortalecer a sua estratégia de segurança, e as notas e quadros fornecem informações práticas ou adicionais.

parte 1

Bastidores

Capítulo 1

O Elo Mais Fraco da Segurança

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe.

Mesmo assim essa empresa ainda estará vulnerável.

Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança.

Esses indivíduos ainda estarão completamente vulneráveis.

O FATOR HUMANO

Ao testemunhar no Congresso há pouco tempo, expliquei que poderia conseguir senhas e outras informações sigilosas nas empresas fingindo ser outra pessoa e *simplesmente pedindo essas informações.*

E natural querer se sentir seguro e isso leva muitas pessoas a buscarem uma falsa idéia de segurança. Veja o caso do responsável e carinhoso proprietário de uma casa que tem um Medico, um cadeado de fechadura conhecido como sendo à prova de roubo, o qual foi instalado na porta da frente para proteger sua esposa, seus filhos e sua casa. Agora ele está certo de que tornou sua família muito mais segura com relação a intrusos. Mas e o intruso que quebra uma janela ou descobre o código que abre a porta da garagem? Que tal instalar um sistema de segurança resistente? Isso é melhor, mas não garante nada. Com cadeados caros ou não, o proprietário da casa permanece vulnerável

Por quê? Porque o fator *humano* é o elo mais fraco da segurança.

Com freqüência, a segurança é apenas uma ilusão, que às vezes fica pior ainda quando entram em jogo a credulidade, a inocência ou a ignorância. O cientista mais respeitado do mundo no século XX, Albert Einstein, disse: "Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro". No final, os ataques da engenharia social podem ter sucesso quando as pessoas são estúpidas ou, em geral, apenas desconhecem as boas práticas da segurança. Com a mesma atitude do nosso proprietário de casa consciente sobre a segurança, muitos profissionais da tecnologia da informação (TI) conservam a idéia errada de que tomaram suas empresas imunes ao ataque porque usaram produtos de segurança padrão — firewalls, sistemas de detecção de intrusos *(Intrusion Detection Systems)* ou dispositivos avançados de autenticação, tais como tokens baseados no tempo ou cartões biométricos inteligentes. Todos que acham que os produtos de segurança sozinhos oferecem a verdadeira segurança estão fadados a sofrer da *ilusão* da segurança, Esse é o caso de viver em um mundo de fantasia: mais cedo ou mais tarde eles serão vítimas de um incidente de segurança.

Como observou o consultor de segurança Bruce Schneier, "a segurança não é um produto, ela é um processo". Além disso, a segurança não é um problema para a tecnologia — ela é um problema para as pessoas e a direção.

A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

UM CASO CLÁSSICO DE FRAUDE

Qual e a maior ameaça à segurança dos bens da sua empresa? Isso é fácil: o engenheiro social, um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos. Esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado.

Dê uma olhada em um exemplo da engenharia social. Não há muitas pessoas hoje que ainda se lembram do jovem chamado Stanley Mark Rifkin e de sua pequena aventura com o agora extinto Security Pacific National Bank, de Los Angeles. Os relatos dessa invasão variam e Rifkin (assim como eu) nunca contou a sua própria versão. Assim sendo, o que vem a seguir se baseia nos relatórios publicados.

Descoberta do código

Certo dia em 1978, Rifkin perambulou pela sala de transferência eletrônica com acesso autorizado apenas para os funcionários do Security Pacific, na qual a equipe enviava e transferia vários bilhões de dólares todos os dias.

Ele trabalhava como contratado de uma empresa que desenvolvia um sistema de backup para os dados da sala de transferência para o caso de seu computador principal ficar paralisado. Essa função deu-lhe acesso aos procedimentos de transferência, incluindo o modo como os funcionários do banco organizavam o envio de uma transferência. Ele aprendeu que os funcionários do banco que estavam autorizados a pedir as transferências eletrônicas recebiam um código diário secreto a cada manhã, o qual era usado quando ligavam para a sala de transferência.

Na sala de transferência, os funcionários nem se davam ao trabalho de memorizar o código de cada dia. Eles escreviam o código em um pedaço de papel e o colocavam em um lugar no qual podiam vê-lo facilmente. Nesse dia de novembro em particular, Rifkin tinha um motivo específico para a sua visita. Ele queria dar uma olhada naquele papel.

Ao chegar à sala de transferência, anotou os procedimentos operacionais, supostamente para ter certeza de que o sistema de backup se combinaria com os sistemas normais. Nesse meio tempo, leu discretamente o código de segurança no pedaço de papel e o memorizou. Alguns minutos depois foi embora. Como declarou mais tarde, ele se sentiu como se houvesse ganhado na loteria.

Há essa conta no banco suíço...

Ao sair da sala lá pelas 3 horas da tarde, ele foi direto para o telefone público no saguão de mármore do prédio, no qual depositou uma ficha e discou para a sala de transferência eletrônica. Em seguida, transformou-se de Stanley Rifkin. consultor do banco, em Mike Hansen, um membro do Departamento Internacional do banco.

Segundo uma fonte, a conversação foi mais ou menos esta:

"Olá, aqui quem fala é Mike Hansen, do Internacional", ele disse para a jovem que atendeu ao telefone.

Ela pediu o número do escritório. Esse era um procedimento padrão e ele estava preparado. "286", respondeu.

A garota continuou, "Muito bem, qual é o código?"

Rifkin disse que nesse ponto o seu coração disparado pela adrenalina "retomou o ritmo". Ele respondeu com calma "4789". Em seguida, deu as instruções para a transferência de "dez milhões e duzentos mil dólares exatamente" para o Irving Trust Company de Nova York, a crédito do Wozchod Handels Bank de Zurique, Suíça, onde ele já havia aberto uma conta.

Em seguida, a garota retrucou: "Muito bem, entendi. Agora preciso do número de estabelecimento entre escritórios."'

Rifkin começou a suar frio; essa era uma pergunta que ele não havia previsto, algo que havia esquecido nos detalhes da sua pesquisa. Mas conseguiu permanecer calmo, agiu como se tudo estivesse bem e respondeu rapidamente: "Eu vou verificar e ligo logo em seguida." Ele ligou para outro departamento do banco, só que desta vez alegou ser um empregado da sala de transferência eletrônica. Ele conseguiu o número de estabelecimento e ligou novamente para a garota.

Ela anotou o número e agradeceu. (Nessas circunstancias o seu agradecimento tem de ser considerado como algo altamente irônico.)

Conseguindo o fechamento

Alguns dias depois, Rifkin voou para a Suíça, pegou o seu dinheiro e trocou mais de US$ 8 milhões com uma agência russa por diamantes. Ele voou de volta e passou pela alfândega americana com as pedras ocultas no cinto de carregar dinheiro. Ele havia dado o maior desfalque bancário da história — e fez isso sem usar uma arma, sequer um computador. O curioso é que sua travessura chegou às páginas do *Guiness Book* na categoria de "a maior fraude de computadores".

Stanley Rifkin usou a arte da fraude — as habilidades e as técnicas que hoje são chamadas de engenharia social. Um planejamento cuidadoso e uma boa conversa foram tudo do que precisou.

E este livro fala disso — das técnicas da engenharia social (nas quais sou especializado) e como se defender contra o seu uso na sua empresa.

A NATUREZA DA AMEAÇA

A história de Rifkin deixa bastante claro como a sua sensação de segurança pode ser enganosa. Incidentes como esse — muito bem, eles podem não ser desfalques de US$ 10 milhões, mas são sempre prejudiciais — acontecem t*odos os dias.* Você pode estar perdendo dinheiro agora mesmo, ou alguém pode estar roubando os planos de novos produtos e você nem sabe disso. Se isso ainda não aconteceu na sua empresa, o problema não é *se* isso acontecerá, mas sim *quando* acontecerá.

Uma preocupação crescente

O Computer Security Institute, em sua pesquisa de 2001 sobre os crimes de computadores relatou que 85% das organizações entrevistadas detectaram quebras na segurança dos computadores nos 12

meses anteriores. Esse *é* um número assustador: apenas 15 entre cem organizações responderam que podiam dizer que não haviam tido uma quebra de segurança durante o ano. Igualmente assustador foi o número de organizações que informaram terem tido prejuízos financeiros devido a quebras na segurança dos computadores: 64%. Bem mais do que metade das organizações havia tido prejuízos financeiros. Tudo isso *em um único ano.*

Por experiência própria, acredito que os números dos relatórios como esse são um pouco exagerados. Suspeito da agenda das pessoas que realizam uma pesquisa. Mas isso não quer dizer que o dano não seja extenso. Ele é, sim. Aqueles que não planejam um incidente de segurança estão planejando o fracasso.

Os produtos comerciais de segurança empregados na maioria das empresas visam principalmente o fornecimento da proteção contra o intruso amador de computadores, assim como as crianças que são conhecidas como script kiddies. Na verdade, esses pretendentes a hackers com software baixado são mais um aborrecimento. Quanto maiores as perdas, mais reais as ameaças vindas de atacantes sofisticados com alvos bem-definidos e motivados pelo ganho financeiro. Essas pessoas concentram-se em um alvo de cada vez e não são como os amadores, que tentam se infiltrar no maior número possível de sistemas. Enquanto os intrusos amadores de computadores apenas buscam a quantidade, os profissionais visam as informações de qualidade e valor

As tecnologias como os dispositivos de autenticação (para fornecer a identidade), o controle de acesso (para gerenciar o acesso aos arquivos e recursos do sistema) e os sistemas de detecção de intrusos (o equivalente eletrônico dos alarmes contra arrombamento) são necessárias para um programa corporativo de segurança. Mesmo assim, hoje em dia é típico de uma empresa gastar mais dinheiro em café do que em medidas de contra-ataque para proteger-se dos ataques à segurança.

Assim como uma mente criminosa não resiste à tentação, a mente do hacker é orientada para encontrar maneiras de burlar as poderosas salvaguardas da tecnologia de segurança. E em muitos casos, eles fazem isso visando às pessoas que usam a tecnologia.

Práticas fraudulentas

Há um ditado popular que diz que um computador seguro é aquele que está desligado. Isso é inteligente, mas é falso: o *hacker* convence alguém a entrar no escritório e ligar aquele computador Um adversário que quer as suas informações pode obtê-las, em geral, usando uma de várias maneiras. Tudo é uma questão de tempo, paciência, personalidade e persistência. É nesse ponto que entra a arte da fraude.

Para anular as medidas de segurança, um atacante, um invasor ou um engenheiro social deve encontrar um modo de enganar um usuário de confiança para que ele revele as informações, ou deve enganar alguém importante para que ele forneça o acesso. Quando os empregados de confiança são enganados, influenciados ou manipulados para revelar informações sigilosas ou para executar ações que criem um buraco na segurança para que o atacante se infiltre, nenhuma tecnologia do mundo pode proteger uma empresa. Assim como os analistas de criptografia podem revelar o texto simples de uma mensagem codificada encontrando um ponto fraco que permita que desviem da tecnologia da criptografia, os engenheiros sociais enganam os seus empregados para desviar da tecnologia da segurança.

ABUSO DE CONFIANÇA

Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente — os traços sociais necessários

para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informaçâo-alvo usando as estratégias e táticas da sua habilidade.

Os tecnologistas experientes têm desenvolvido soluções de segurança da informação para minimizar os riscos ligados ao uso dos computadores, mas mesmo assim deixaram de fora a vulnerabilidade mais significativa: o fator humano, Apesar do nosso intelecto, nós humanos — você, eu e todas as outras pessoas — continuamos sendo a ameaça mais séria à segurança do outro.

O nosso caráter nacional

Não temos consciência da ameaça, em particular no mundo ocidental, Nos Estados Unidos, não somos treinados para suspeitarmos uns dos outros. Somos ensinados a "amar o próximo" e ter confiança e fé uns nos outros. Veja como é difícil para as organizações de vigilância de vizinhança fazer com que as pessoas tranquem suas casas e seus carros. Esse tipo de vulnerabilidade é óbvio, e mesmo assim parece ser ignorado por muitas pessoas que preferem viver em um mundo de sonhos — até se queimarem.

Sabemos que nem todas as pessoas são gentis e honestas, mas vivemos como se elas fossem. Essa adorável inocência tem sido a estrutura da vida americana e é doloroso desistir dela, Como uma nação, incorporamos ao nosso conceito de liberdade a idéia de que o melhor lugar para viver é aquele sem cadeados e chaves,

A maioria das pessoas supõe que não será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa; o atacante, entendendo isso como uma crença comum, faz a sua solicitação soar tão razoável que não levanta suspeita enquanto explora a confiança da vítima.

Inocência organizacional

Essa inocência que faz parte do nosso caráter nacional ficou evidente quando os computadores foram conectados remotamente pela primeira vez. Lembre-se de que a ARPANet (a Rede da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa), a antecessora da Internet, foi criada como um modo de compartilhar informações de pesquisa entre o governo e as instituições de pesquisa e educacionais. O objetivo era a liberdade de informações, bem como o avanço tecnológico. Muitas instituições educacionais, portanto, configuraram os primeiros sistemas de computadores com pouca ou nenhuma segurança, Um libertário famoso dos computadores, Richard Stallman, até se recusou a proteger a sua conta com uma senha.

Mas com a Internet sendo usada para o comércio eletrônico, os perigos da pouca segurança do nosso mundo eletrônico mudaram muito. O emprego de mais tecnologia não vai solucionar o problema da segurança humana,

Basta dar uma olhada em nossos aeroportos hoje, A segurança tornou-se imperativa e mesmo assim somos surpreendidos com notícias de passageiros que conseguiram burlar a segurança e passar com armas pelos pontos de checagem. Como isso é possível em uma época na qual os nossos aeroportos estão em tal estado de alerta? Os detectores de metal estão falhando? Não. O problema não são as máquinas, mas o fator humano: as pessoas que operam a máquina. Os funcionários dos aeroportos podem dirigir a Guarda Nacional e instalar detectores de metal e sistemas de reconhecimento facial, mas a educação da equipe de frente da segurança sobre como examinar adequadamente os passageiros pode ajudar muito mais,

O mesmo problema existe dentro do governo, das empresas e das instituições educacionais de todo o mundo, Apesar dos esforços dos profissionais de segurança, as informações em toda a parte

permanecem vulneráveis e continuarão sendo vistas como um alvo pelos atacantes que têm habilidades de engenharia, até que o elo mais fraco da cadeia de segurança, o elo humano, seja fortalecido,

Agora mais do que nunca devemos aprender a parar de ser otimistas e nos tornarmos mais conscientes das técnicas que estão sendo usadas por aqueles que tentam atacar a confidencialidade, integridade e disponibilidade das informações dos nossos sistemas e redes de computadores. Nós acostumamo-nos a aceitar a necessidade da direção segura; agora está na hora de aceitar e aprender a prática da computação defensiva.

A ameaça de uma invasão que viola a nossa privacidade, a nossa mente ou os sistemas de informações da nossa empresa pode não parecer real até que aconteça. Para evitar tamanha dose de realidade precisamos nos conscientizar, educar, vigiar e proteger os nossos ativos de informações, as nossas informações pessoais e as infra-estruturas críticas da nossa nação. E devemos implementar essas precauções hoje mesmo.

TERRORISTAS E FRAUDE

E óbvio que a fraude não é uma ferramenta exclusiva do engenheiro social. O terrorismo físico é mais noticiado e tivemos de reconhecer como nunca antes que o mundo é um lugar perigoso. Afinal de contas, a civilização é apenas um verniz superficial.

Os ataques a Nova York e Washington, D.C, em setembro de 2001, infundiram tristeza e medo nos corações de cada um de nós — não apenas nos americanos, mas também em todas as pessoas bem-intencionadas de todas as nações. Agora estamos alertas para o fato de que há terroristas obcecados localizados em todo o planeta, bem treinados e aguardando para lançar outros ataques contra nós.

O esforço recentemente intensificado do nosso governo aumentou os níveis de nossa consciência de segurança. Precisamos permanecer alertas, em guarda contra todas as formas de terrorismo e entender como os terroristas criam identidades falsas, como assumem os papéis de alunos e vizinhos e se misturam à multidão. Eles mascaram suas crenças verdadeiras enquanto conspiram contra nós — praticando truques de fraude semelhantes àqueles que você verá nestas páginas.

Embora até onde eu saiba os terroristas ainda não usaram as artimanhas da engenharia social para se infiltrarem nas corporações, nas estações de tratamento de água, nas instalações de geração de eletricidade ou em outros componentes vitais da nossa infra-estrutura nacional, o potencial para isso existe. E isso é muito fácil. A consciência de segurança e as políticas de segurança que espero sejam colocadas em prática e implantadas pelo gerenciamento corporativo de primeiro escalão por causa deste livro não virão cedo demais.

SOBRE ESTE LIVRO

A segurança corporativa é uma questão de equilíbrio. Pouca ou nenhuma segurança deixa a sua empresa vulnerável, mas uma ênfase exagerada atrapalha a realização dos negócios e inibe o crescimento e a prosperidade da empresa. O desafio é atingir um equilíbrio entre a segurança e a produtividade.

Outros livros sobre segurança corporativa concentram-se na tecnologia de hardware e software e não abordam adequadamente a ameaça mais séria de todas: a fraude humana. A finalidade aqui *é* ajudá-lo a entender como você, seus colegas e as outras pessoas da sua empresa estão sendo manipulados e ensiná-lo a erguer as barreiras para pararem de ser vítimas. O livro concentra-se principalmente nos métodos não técnicos que os invasores hostis usam para roubar informações, comprometer a integri-

dade das informações que se acredita estarem seguras, mas que não estão, ou para destruir o produto de trabalho da empresa.

A minha tarefa torna-se mais difícil por causa de uma única verdade; cada leitor terá sido manipulado pelos maiores especialistas de todos os tempos da engenharia social — seus pais. Eles encontraram maneiras de fazer com que você — "para o seu próprio bem" — fizesse aquilo que achavam ser o melhor Os pais tomam-se os grandes contadores de histórias da mesma forma que os engenheiros sociais desenvolvem com habilidade cada uma das histórias plausíveis, dos motivos e das justificativas para atingir seus objetivos. Sim, todos fomos moldados por nossos pais: benevolentes (e, às vezes, nem tanto) engenheiros sociais.

Condicionados por aquele treinamento, tornamo-nos vulneráveis á manipulação. Teríamos uma vida difícil se tivéssemos de estar sempre em guarda e desconfiando dos outros, preocupados com o fato de sermos feitos de bobos por alguém que está tentando se aproveitar de nós. Em um mundo perfeito, confiaríamos implicitamente nos outros, certos de que as pessoas que encontramos serão honestas e confiáveis. Mas não vivemos em um mundo perfeito e, portanto, temos de exercer um padrão de vigilância para repelir os esforços fraudulentos dos nossos adversários.

As principais partes deste livro, as Partes 2 e 3, são formadas por histórias que mostram os engenheiros sociais em ação. Nessas seções, você lerá sobre:

- O que os phreaks (hackers da telefonia) descobriram há anos: um método simples para obter um número de telefone não relacionado na empresa de telefonia.
- Vários métodos diferentes usados pelos atacantes para convencer até mesmo os empregados alertas e desconfiados a revelarem seus nomes de usuário e as senhas de computador
- Como um gerente do Centro de Operações cooperou para permitir que um atacante roubasse as informações de produto mais secretas da sua empresa.
- Os métodos de um atacante que enganou uma senhora para baixar software que espia cada tecla que ela digita e envia os detalhes por e-mail para ele.
- Como os detetives particulares obtêm as informações sobre a sua empresa e sobre você, e posso garantir que isso fará você sentir um arrepio na espinha.

Você pode achar que as histórias das Partes 2 e 3 não são possíveis, que ninguém poderia ter sucesso com as mentiras, com os truques sujos e os esquemas descritos. A verdade é que, em cada um desses casos, as histórias descrevem eventos que podem acontecer e acontecem; muitas delas estão acontecendo todos os dias em algum lugar do planeta, talvez até mesmo estejam acontecendo na sua empresa enquanto você está lendo.

Essas informações abrirão seus olhos para que você proteja a sua empresa, rebata os avanços de um engenheiro social e proteja a integridade das informações na sua vida privada.

Na Parte 4, mudo de assunto. O meu objetivo aqui é ajudar você a criar as políticas de negócios e o treinamento em conscientização necessários para minimizar as chances de seus empregados serem enganados por um engenheiro social. O entendimento das estratégias, dos métodos e das táticas do engenheiro social o ajudará a preparar-se para empregar controles razoáveis que salvaguardam os seus ativos de TI, sem afetar a produtividade da sua empresa.

Em resumo, escrevi este livro para aumentar a sua conscientização sobre a séria ameaça representada pela engenharia social e para ajudá-lo a ter certeza de que a sua empresa e seus empregados têm menos chances de serem explorados dessa maneira.

Ou, quem sabe, devesse dizer bem menos chances de serem explorados *novamente,*

parte 2

A Arte do Atacante

Capítulo 2

Quando as Informações Não São Inofensivas

De acordo com a maioria das pessoas, qual é a verdadeira ameaça dos engenheiros sociais? O que você deve fazer para se proteger?

Se o objetivo é capturar algum prêmio altamente valioso — digamos um componente vital do capital intelectual da empresa —, então talvez você precise, no sentido figurado, apenas de um cofre mais forte e de guardas mais armados. Certo?

Mas na verdade a invasão da segurança de uma empresa quase sempre começa com o cara mau obtendo alguma informação ou algum documento que parece ser muito inocente, tão comum e sem importância que a maioria das pessoas da organização não vê nenhum motivo pelo qual ele deva ser protegido e restrito.

O VALOR OCULTO DAS INFORMAÇÕES

Grande parte das informações aparentemente inócuas de posse de uma empresa é cobiçada por ura atacante da engenharia social porque ela pode ter um papel vital em seu esforço de se revestir de credibilidade.

Em todas estas páginas, mostro como os engenheiros sociais fazem o que fazem permitindo que você "testemunhe" os ataques por si mesmo — apresentando a ação sob o ponto de vista das vítimas e permitindo que você coloque-se em seu lugar e meça como você mesmo (ou talvez um dos seus empregados ou colegas) teria respondido. Em muitos casos, você também experimentará os mesmos eventos sob a perspectiva do engenheiro social.

A primeira história examina a vulnerabilidade na indústria financeira.

CREDITCHEX

Durante muito tempo, os britânicos conviveram com um sistema bancário muito conservador, Como um cidadão comum, você não podia atravessar a rua e abrir uma conta no banco. Não, o banco nem pensaria em aceitá-lo como cliente, a menos que algum cliente já bem estabelecido lhe fornecesse uma carta de recomendação.

Isso é muito diferente do aparentemente igualitário sistema bancário de hoje. Em nenhum outro lugar a nossa moderna facilidade de fazer negócios está em mais evidência do que na América demo-

crática e amistosa, na qual quase todos podem entrar em um banco e abrir facilmente uma conta corrente, certo? Bom, as coisas não são bem assim. A verdade é que os bancos tem uma compreensível relutância natural em abrir uma conta para alguém que pode ter um histórico de emitir cheques sem fundo — isso seria como dar as boas-vindas a uma folha corrida de roubos a banco e condenações por desfalques. Assim sendo, muitos bancos adotam a prática padrão de atribuir polegares para cima ou para baixo para um possível novo cliente.

Uma das principais empresas que os bancos contratam para obter essas informações *é* um local que chamaremos de CreditChex. Elas fornecem um serviço valioso a seus clientes, mas, assim como muitas empresas, também podem fornecer sem querer um serviço útil para os engenheiros sociais bem informados.

A primeira ligação: Kim Andrews

"National Bank, Kim. Você quer abrir uma conta hoje?"

"Olá, Kim. Eu quero fazer uma pergunta. Vocês usam a CreditChex?"

"Sim."

"Quando vocês ligam para a CreditChex, como você chama o número que fornece — um MD do Comerciante'"?

Há uma pausa; ela está pensando na pergunta, perguntando-se do que se trata e se ela deve responder.

O interlocutor continua rapidamente sem perder o ritmo: "Sabe, Kim. estou escrevendo um livro. Ele trata de investigações particulares."

"Sim", ela diz, respondendo à pergunta com confiança e feliz em ajudar um escritor.

"Então vocês chamam esse número de ID do comerciante, não é?"

"Hum, hum."

"Ótimo, porque eu queria ter certeza de que estava usando a linguagem certa no livro. Obrigado pela sua ajuda. Até logo, Kim."

A segunda ligação: Chris Talbert

"National Bank, Contas Novas, Chris".

"Olá, Chris. Aqui é o Alex", o interlocutor diz. "Eu sou um representante do serviço ao cliente da CreditChex. Estamos fazendo uma pesquisa para melhorar os nossos serviços. Você tem alguns minutos?"

Ela concordou e o interlocutor continua:

"Muito bem — qual o horário de funcionamento da sua filial?" Ela respondeu e continuou respondendo às suas perguntas.

"Quantos empregados da sua filial usam o nosso serviço?"

"Com que freqüência você liga para nós com uma consulta?"

"Qual dos nossos números 800 nós designamos para vocês usarem ao ligar para nós?"

"Os nossos representantes são sempre educados?"

"Qual é o nosso tempo de resposta?"

"Há quanto tempo você trabalha no banco?"

"Qual ID de Comerciante você está usando no momento?"

"Você já encontrou alguma imprecisão nas informações que fornecemos?"

"Se você tivesse alguma sugestão para melhorar o nosso serviço, qual seria?"

E finalmente:

"Você se importaria em preencher questionários periódicos se os enviássemos para a sua filial?"

Ela concordou, eles conversaram um pouco, o interlocutor desligou e Chris voltou ao trabalho.

A terceira ligação: Henry McKinsey

"CreditChex, Henry McKinsey, posso ajudar?"

O interlocutor disse que ele era do National Bank, Ele deu o ID de Comerciante adequado e. em seguida, o nome e o número do seguro social da pessoa de quem ele queria informações. Henry pediu a data de nascimento e o interlocutor forneceu-a também.

Após alguns instantes, Harry leu a listagem na tela do seu computador.

'Wells Fargo informou NSF em 1998, uma vez, valor de US$ 2.066." NSF — fundos insuficientes — é a linguagem conhecida para os cheques que foram passados sem que houvesse dinheiro em conta para a sua compensação.

"Alguma atividade desde então?"

"Nenhuma atividade."

"Houve outras consultas?"

"Vejamos. Sim, duas e ambas no último mês. A terceira no United Credit Union, de Chicago." Ele parou no próximo nome, Schenectady Mutual Investments, e teve de soletrá-lo. "Isso é no Estado de Nova York", ele acrescentou.

O detetive particular em ação

Todas aquelas três ligações foram feitas pela mesma pessoa: um detetive particular que chamaremos de Oscar Grace. Grace tinha um cliente novo, um de seus primeiros clientes. Ele era tira há alguns meses e descobriu que parte desse novo trabalho veio naturalmente, mas outra parte representava um desafio para os seus recursos e a sua criatividade.

Esse cliente classificava-se sem dúvida na categoria do desafio. Os insensíveis olhos privados da ficção — os Sam Spades e os Philip Marlowes — passaram madrugadas sentados em carros observando uma esposa infiel. Os detetives da vida real fazem o mesmo. Eles também fazem coisas sobre as quais não se escreve tanto, mas um tipo não menos importante de espionagem de esposas, um método que depende mais das habilidades de engenharia social do que da luta contra o aborrecimento das vigílias na madrugada.

O novo cliente de Grace era uma senhora que parecia ter um orçamento bastante grande para roupas e jóias. Ela entrou certo dia no seu escritório e sentou-se na cadeira de couro, a única que não tinha papéis empilhados. Ela colocou a sua bolsa Gucci na mesa com o logotipo virado para ele e anunciou que pretendia dizer ao marido que queria se divorciar, mas admitia ter "apenas um probleminha".

Parece que o seu marido estava um passo adiante. Ele já havia sacado o dinheiro de sua conta poupança e uma soma maior ainda da sua conta em uma corretora. Ela queria saber o destino do seu patrimônio e o advogado do seu divórcio não estava ajudando muito. Grace conjecturou que o advogado era um daqueles conselheiros de altos salários que não queriam sujar as mãos com algo tão complicado quanto saber aonde foi parar o dinheiro.

Será que Grace poderia ajudar?

Ele garantiu que isso seria fácil, fez uma cotação para o serviço, fora as despesas, e recebeu um cheque como primeiro pagamento.

Em seguida, ele enfrentou o seu problema. O que você faria se nunca tivesse feito um trabalho assim antes e não soubesse muito bem por onde começar a rastrear o dinheiro? Você avança a passos de bebê. Aqui, de acordo com a nossa fonte, está a história de Grace.

Eu conhecia o CreditChex e o modo como os bancos o usavam — a minha ex-mulher trabalhava em um banco. Mas não sabia qual era o jargão e os procedimentos e seria perda de tempo tentar perguntar isso a ela.

Etapa um: Aprenda a terminologia e descubra como fazer a solicitação para que pareça que você sabe do que está falando. No banco para o qual liguei, a primeira jovem, Kim, desconfiou quando perguntei sobre como eles se identificavam quando ligavam para o CreditChex. Ela hesitou; não sabia se devia contar isso para mim. Fui derrotado por isso? Nem um pouco. Na verdade, a hesitação me deu uma pista importante, um sinal de que eu tinha de fornecer um motivo para que ela acreditasse. Quando apliquei a mentira de que estava fazendo pesquisas para um livro, ela relaxou. Você diz que é um escritor ou roteirista e todas as portas se abrem.

Ela tinha outro conhecimento que teria ajudado — coisas como quais informações o CreditChex requer para identificar a pessoa sobre a qual você está querendo as informações, quais informações você pode pedir e a maior delas: qual era o número de ID de Comerciante do banco de Kim. Eu estava pronto para fazer aquelas perguntas, mas a sua hesitação enviou um sinal vermelho. Ela acreditou na história da pesquisa para um livro, mas já tinha algumas suspeitas. Se tivesse sido mais receptiva desde o início, eu teria pedido para que ela revelasse mais detalhes sobre seus procedimentos.

Você tem de confiar em seus instintos, ouvir com atenção o que o *Mark* está dizendo e como ele está dizendo isso. Essa moça parecia ser bastante inteligente para ouvir o alarme quando fizesse muitas perguntas incomuns. E embora ela não soubesse quem eu era e de qual número eu estava falando, mesmo assim nesse negócio você nunca quer que alguém espalhe que está procurando alguém e liga para obter informações sobre os negócios. Isso acontece porque você não quer *queimar a fonte* — você pode ligar novamente para o mesmo escritório em outra ocasião.

Jargão

MARK A vítima de uma conspiração.

QUEIMAR A FONTE Diz-se que um atacante queimou a fonte quando ele permite que uma vitima reconheça que ocorreu um ataque. Após a vítima tomar conhecimento e notificar os outros empregados ou a direção sobre a tentativa, fica muito difícil explorar a mesma fonte em ataques futuros.

Sempre observo os pequenos sinais que me dão uma leitura da cooperação de uma pessoa, em uma escala que vai desde "Você parece uma boa pessoa e acredito em tudo que você está dizendo" até "Ligue para a polícia, chame a Polícia Federal, essa pessoa não está querendo boa coisa".

Entendi que Kim estava um pouco em dúvida, assim, liguei para alguém de uma filial diferente. Na minha segunda ligação com Chris, o truque da pesquisa a encantou. A tática aqui é incluir as perguntas importantes entre aquelas sem conseqüências que são usadas para criar uma idéia de credibilidade. Antes de entrar com a pergunta sobre o número do ID de Comerciante do CreditChex, fiz um pequeno teste de última hora fazendo uma pergunta pessoal sobre há quanto tempo ela trabalhava no banco.

Uma pergunta pessoal e como um campo minado — algumas pessoas pisam sobre uma mina e nunca percebem; no caso de outras pessoas, a mina explode e faz com que elas saiam correndo em busca de segurança. Assim sendo, se eu fizer uma pergunta pessoal, ela responder a pergunta e o tom da sua voz não mudar, isso significa que provavelmente ela não é cética sobre a natureza da solicitação. Posso seguramente fazer a pergunta que estou querendo sem levantar suas suspeitas, e ela talvez me dará a resposta que desejo.

Mais uma coisa que um bom detetive particular sabe: nunca encerre uma conversação após obter a informação-chave. Outras duas ou três perguntas, um pouco de bate-papo e então pode dizer adeus. Mais tarde, se a vítima se lembrar de alguma coisa que você perguntou, provavelmente ela se lembrará das últimas perguntas. O restante em geral será esquecido.

Assim, Chris me deu o seu número de ID de Comerciante e o número de telefone que eles ligam para fazer as solicitações, Eu ficaria mais feliz se tivesse feito algumas perguntas sobre quantas informações *é* possível obter da CreditChex. Mas achei melhor não abusar da minha sorte.

Isso era como ter um cheque em branco da CreditChex. Agora eu podia ligar e obter informações sempre que quisesse. E nem tinha de pagar pelo serviço. O representante da CreditChex ficou satisfeito em compartilhar exatamente das informações que eu queria; os dois lugares nos quais o marido da minha cliente havia se inscrito recentemente para abrir uma conta. Assim sendo, onde estavam os bens que a sua futura ex-mulher estava procurando? Onde mais além das instituições bancárias que o funcionário da CreditChex relacionou?

Recado do Mitnick

Um ID de Comerciante nessa situação é como uma senha. Se o pessoal do banco o tratasse como uma senha de caixa eletrônico, eles poderiam apreciar a natureza delicada das informações. Há algum código interno ou um número na sua organização que não esteja sendo tratado com cuidado suficiente pelas pessoas?

Analisando a trapaça

Todo esse ardil baseou-se em uma das táticas fundamentais da engenharia social: ganhar acesso ás informações que o empregado de uma empresa trata como inofensivas, quando na verdade elas não são.

A primeira funcionária do banco confirmou a terminologia para descrever o número de identificação usado ao ligar para o CreditChex: o ID de Comerciante. A segunda forneceu o número de telefone para ligar para o CreditChex e a informação mais vital: o número de ID de Comerciante. Todas essas informações pareciam ser inofensivas para a funcionária. Afinal de contas, ela achou que estava falando com alguém do CreditChex — e assim, qual seria o mal de divulgar o número?

Tudo isso criou a base para a terceira ligação. Grace tinha tudo o que precisava para ligar para a CreditChex, para se passar como representante de um de seus bancos clientes, o National, e simplesmente pedir as informações que estava querendo.

Com habilidades para roubar informações tão boas quanto aquelas que um trapaceiro tem para roubar o seu dinheiro, Grace tinha talentos bem treinados para ler as pessoas. Ele conhecia a tática comum de esconder as principais perguntas entre aquelas mais inocentes. Ele sabia que uma pergunta pessoal testaria a disposição da segunda funcionária em cooperar antes de pedir inocentemente o número do ID de Comerciante.

O erro do primeiro funcionário ao confirmar a terminologia para o número do ID do CreditChex foi um erro quase impossível de ser evitado. As informações são tão conhecidas dentro da indústria bancária que elas parecem não ter importância — o próprio modelo da inocência. Mas a segunda funcionária, Chris, não deveria ter sido tão disposta a responder perguntas sem verificar se o interlocutor era de fato quem dizia ser Ela deveria pelo menos ter anotado seu nome e número e ter ligado novamente. Dessa forma, se mais tarde surgisse alguma dúvida, ela teria um registro do número do telefone usado pela pessoa. Neste caso, uma ligação como essa tomaria muito mais difícil para o atacante disfarçar-se de representante do CreditChex.

Teria sido melhor ainda ligar para o CreditChex usando um número que o banco já tinha em seus registros — não um número fornecido pelo interlocutor — para verificar se a pessoa realmente trabalhava lá, e se a empresa eslava realmente fazendo uma pesquisa com os clientes. Dados os detalhes práticos do mundo real e as pressões de tempo sob as quais a maioria das pessoas trabalha hoje em dia. seria muito esperar esse tipo de ligação telefônica de verificação, exceto quando um empregado suspeita de que algum tipo de ataque está sendo realizado,

A ARMADILHA DE ENGENHEIRO

E de conhecimento geral que as empresas caça-talentos usam as táticas da engenharia social para recrutar talentos corporativos. Este é um exemplo de como isso pode acontecer.

No final dos anos de 1990, uma agência de empregos não muito ética conseguiu um cliente novo, uma empresa que estava procurando engenheiros elétricos com experiência na indústria de telefonia, O pivô do projeto era uma senhora dotada de uma voz rouca e um modo *sexy* que ela havia aprendido a usar para desenvolver a confiança inicial e afinidade pelo telefone.

A senhora resolveu atacar um provedor de serviços de telefonia celular para saber se ela poderia localizar alguns engenheiros que estivessem tentados a atravessar a rua e ir trabalhar para um concorrente. Ela não podia ligar para a telefonista e dizer "Quero falar com alguém que tenha cinco anos de experiência como engenheiro". Em vez disso, por motivos que ficarão claros em alguns instantes, ela começou o assalto aos talentos buscando uma informação que parecia não ser nada sigilosa, uma informação que a empresa dá para quase todas as pessoas que a pedem.

A primeira ligação: a recepcionista

Usando o nome Didi Sands, a atacante fez uma ligação para os escritórios da empresa de telefonia celular. Esta foi parte da conversação:

Recepcionista: Boa tarde. Sou Marie. posso ajudar?

Didi: Você pode me passar para o Departamento de Transportes?

R: Eu não sei se temos um, vou procurar na minha listagem. Com quem falo?

D: Aqui é Didi.

R: Você está ligando do prédio ou.,.?

D: Não, eu estou fora do prédio.

R: Didi de quê?

D: Didi Sands. Eu tinha o ramal de Transportes, mas esqueci.

R: Um momento.

Para evitar suspeitas, nesse ponto Didi fez uma pergunta casual só para manter a conversação, com a intenção de estabelecer o fato de que ela estava "por dentro" e familiarizada com as localizações da empresa.

D: Em qual prédio você está — Lakeview ou Main Place?

R: Main Place. (pausa) O número é 805 555 6469.

Para ter um backup caso a ligação para Transportes não fornecesse aquilo que ela estava procurando, Didi disse que ela também queria falar com Imóveis. A recepcionista deu esse número também. Quando Didi pediu para ser transferida para Transportes, a recepcionista tentou, mas a linha estava ocupada.

Nesse ponto, Didi pediu um *terceiro* número de telefone, o de Contas a Receber, o qual estava localizado em um prédio corporativo em Austin, no Texas. A recepcionista pediu para ela aguardar um momento e saiu da linha. Ela estava consultando a Segurança dizendo que estava com uma ligação telefônica suspeita e achou que havia algo de estranho. De forma alguma, responderam, e Didi não teve a menor preocupação. Ela estava ficando meio aborrecida, mas para a recepcionista isso tudo fazia parte de um dia normal de trabalho. Após cerca de um minuto, a recepcionista voltou à linha procurou o número de Contas a Receber, fez a transferência e colocou Didi na linha.

A segunda ligação: Peggy

A próxima conversação foi assim:

Peggy: Contas a Receber, Peggy.

Didi: Oi, Peggy. Aqui é Didi, de Thousand Oaks.

P: Oi, Didi.

D: Como vai?

P: Tudo bem.

Em seguida, Didi usou um termo familiar no mundo corporativo que descreve o código de cobrança para designar as despesas no orçamento de uma organização ou grupo de trabalho específico:

D; Excelente. Tenho uma pergunta. Como encontro o centro de custo de determinado departamento?

P; Você tem de falar com o analista de orçamento do departamento.

D: Você sabe quem é o analista de orçamento para Thousand Oaks — a sede? Eu estou tentando preencher um formulário e não sei qual é o centro de custo apropriado.

P: Só sei que quando você precisa do número do centro de custo, você liga para o seu analista de orçamento.

D: Você tem um centro de custo no seu departamento ai no Texas?

P: Temos o nosso próprio centro de custo, mas eles não nos dão a lista com todos eles.

D: Quantos dígitos tem o centro de custo? Por exemplo, qual é o seu centro de custo?

P: Bem, você trabalha no 9WC ou no SAT?

Didi não tinha a menor idéia de quais eram esses departamentos ou grupos, mas isso não importava. Ela respondeu:

D: 9WC.

P: Então em geral são quatro dígitos. Onde você disse que trabalhava?

D: Na sede em Thousand Oaks.

P: Bem, aqui tem um para Thousand Oaks, Ê 1A5N, com N de Nancy.

Falando apenas o tempo suficiente com alguém que estava disposto a ajudar, Didi conseguiu o número do centro de custo de que precisava — uma daquelas informações que ninguém pensa em proteger, porque parece algo que nunca terá valor para uma pessoa de fora.

A terceira ligação: um número errado útil

A próxima etapa para Didi seria explorar o número do centro de custo e transformá-lo em algo de valor verdadeiro, usando-o como uma ficha de pôquer.

Ela começou ligando para o departamento de Imóveis fingindo ter ligado para um número errado. Começando com um "Desculpe incomodar, mas...", ela disse que era uma funcionária que havia perdido a lista de telefones da empresa e perguntou para quem ela deveria ligar para conseguir uma outra cópia. O homem disse que a cópia impressa estava desatualizada, porque ela estava disponível no site da intranet da empresa.

Didi disse que preferia usar uma cópia impressa e o homem disse para ela ligar para Publicações e, em seguida, sem que ela pedisse — talvez só para manter a senhora com voz *sexy* mais um pouco na linha — procurou o número e o forneceu para ela.

A quarta ligação: Bart, em Publicações

Em Publicações, ela falou com um homem chamado Bart. Didi disse que era de Thousand Oaks e que eles tinham um consultor novo que precisava de uma cópia da lista de telefones da empresa. Ela disse que uma cópia impressa funcionaria melhor para o consultor, mesmo que estivesse meio desatualizada. Bart disse que ela teria de preencher um formulário de requisição e enviá-lo para ele.

Didi disse que estava sem formulários e com muita pressa, e perguntou se Bart não poderia fazer o favor de preencher o formulário para ela. Ele concordou, não muito entusiasmado, e Didi forneceu os detalhes. Como endereço da contratada fictícia, ela deu o número daquilo que os engenheiros sociais chamam de *rnail drop,* o qual, nesse caso, era uma empresa de caixas postais na qual a sua empresa alugava caixas postais para situações como aquela.

A preliminar anterior tornou-se útil agora: seria cobrada uma taxa pelo custo e envio da lista. Muito bem — Didi deu o centro de custo de Thousand Oaks:

"1A5N, com N de Nancy".

Jargão

MAIL DROP O termo do engenheiro social para uma caixa postal alugada, em geral com um nome fictício, a qual é usada para o recebimento de documentos ou pacotes que a vítima foi convencida a enviar.

Alguns dias depois, quando chegou a lista de telefones corporativos, Didi descobriu que isso valia mais a pena do que ela havia imaginado: ela não apenas tinha os nomes e números de telefones, mas também quem trabalhava para quem — a estrutura corporativa de toda a organização.

A senhora de voz forte estava pronta para começar a caçar o seu talento e fazer ligações telefônicas em busca de pessoas. Ela havia trapaceado as informações que precisava ter para iniciar o seu ataque usando o dom da palavra lapidado ao máximo que cada engenheiro social habilidoso tem. Agora ela estava pronta para receber a recompensa.

Recado do Mitnick

Assim como as peças de um quebra-cabeça, cada informação parece irrelevante sozinha. Porém, quando as peças são juntadas, uma figura aparece. Neste caso, a figura do engenheiro social mostrou toda a estrutura interna da empresa.

Analisando a trapaça

Neste ataque da engenharia social, Didi começou conseguindo os telefones dos três departamentos da empresa-alvo. Isso foi fácil, os números que ela queria não eram segredo, particularmente para os empregados. Um engenheiro social aprende a se fazer passar por alguém de dentro da empresa e Didi fazia isso com habilidade,

Um dos números de telefone a levaram a um número de centro de custo, o qual foi usado em seguida para obter uma cópia da lista de telefones dos funcionários da empresa.

As principais ferramentas que ela precisava ter: parecer amistosa, usar um pouco do jargão corporativo e, com a última vítima, jogar um pouco de areia nos olhos dos outros.

E mais uma ferramenta, um elemento essencial que não pode ser adquirido facilmente — as habilidades de manipulação do engenheiro social refinadas por meio de extensa prática e as lições não escritas pelas gerações de homens de confiança.

MAIS INFORMAÇÕES "VALIOSAS"

Alem de um número de centro de custo e dos ramais dos telefones internos, quais outras informações aparentemente inúteis podem ser valiosíssimas para o seu inimigo?

Ligação telefônica para Peter Abel

"Oi", a voz no outro lado da linha diz. "Sou Tom. da Parkhurst Travel. As suas passagens para São Francisco estão prontas. Você quer que as entreguemos ou vai retirá-las?"

"São Francisco?", diz Peter. "Eu não vou para São Francisco."

"O senhor é Peter Abeis?"

"Sim, mas eu não tenho nenhuma viagem programada."

"Bem", disse o interlocutor com uma risada amistosa, Você tem certeza de que não quer ir a São Francisco?",

"Se você acha que pode convencer o meu chefe... ", retruca Peter, brincando com a conversa amistosa.

"Parece que houve alguma confusão", salienta o interlocutor, "No nosso sistema, tomamos as providências de viagem pelo número de empregado. Talvez alguém tenha usado o número errado. Qual é o seu número de empregado?"

Peter informa o seu número. E por que não? Ele aparece em quase todos os formulários pessoais que preenche, muitas pessoas da empresa têm acesso a ele — recursos humanos, folha de pagamento e, obviamente, a agência externa de viagens. Ninguém trata um número de empregado como um segredo. Que diferença faria?

A resposta não é difícil de descobrir. Duas ou três informações seriam o suficiente para montar uma farsa efetiva — o engenheiro social usando a identidade de outra pessoa. Consiga o nome de um empregado, o seu número de telefone, o seu número de empregado, e quem sabe também o nome e número de telefone do seu gerente, e um engenheiro social a caminho de ser competente tem a maior parte daquilo que ele precisa para parecer autêntico para o próximo alvo.

Se alguém dizendo que era de outro departamento dentro da sua empresa ligasse ontem, desse um motivo plausível e pedisse o seu número de empregado, você relutaria em dar-lhe a informação?

E por falar nisso, qual é o seu número de seguro social?

Recado do Mitnick

A moral da história é: não dê nenhuma informação pessoal ou interna da empresa, nem identificadores para ninguém, a menos que a sua voz seja conhecida e o solicitante tenha necessidade de saber a informação.

EVITANDO A TRAPAÇA

A sua empresa tem a responsabilidade de informar os empregados sobre como pode ocorrer um erro sério quando informações não públicas são tratadas da forma errada. Uma política de segurança bem desenvolvida, combinada à educação e treinamento adequados, aumenta bastante a consciência do empregado sobre o tratamento correto das informações comerciais corporativas. Uma política de classificação de dados ajuda você a implementar os controles adequados para a divulgação das informações. Sem uma política de classificação de dados, todas as informações internas devem ser consideradas confidenciais, a menos que seja especificado o contrário.

Use estas etapas para proteger a sua empresa contra a divulgação de informações aparentemente inofensivas:

- O Departamento de Segurança das Informações precisa realizar o treinamento da conscientização, o qual detalha os métodos usados pelos engenheiros sociais. O método descrito an-

teriormente é 3 obtenção de informações aparentemente não sigilosas e o seu uso como uma ficha de pôquer para ganhar a confiança de curto prazo. Cada um dos empregados precisa ter consciência de que o falo de um interlocutor ter conhecimento dos procedimentos da empresa, da linguagem e dos identificadores internos não dá de maneira nenhuma a forma ou a autenticação para o solicitante, nem o autoriza a ter a necessidade de saber as informações. Um interlocutor pode ser um ex-empregado ou contratado com as informações internas requisitas. Da mesma forma, cada corporação tem a responsabilidade de determinar o método apropriado de autenticação a ser usado quando os empregados interagem com as pessoas que eles não conhecem pessoalmente ou pelo telefone.

A pessoa ou as pessoas que têm o papel e a responsabilidade de criar uma política de classificação de dados devem examinar os tipos de detalhes que parecem inofensivos e podem ser usados para obter o acesso dos empregados legítimos, mas esses detalhes podem levar a informações sigilosas. Embora você nunca daria os códigos de acesso do seu cartão eletrônico, diria a alguém qual servidor você usa para desenvolver produtos de software para a empresa? Essas informações poderiam ser usadas por uma pessoa que finge ser outra que tem acesso legítimo a rede corporativa?

O simples conhecimento da terminologia interna pode fazer com que um engenheiro social pareça assumir autoridade e conhecimento. O atacante quase sempre usa esse erro comum de conceito para fazer com que suas vítimas colaborem. Por exemplo, um ID de Comerciante é um identificador que as pessoas do departamento de Contas Novas de um banco usam todos os dias. Mas tal identificador é exatamente igual a uma senha. Se cada um dos empregados entender a natureza desse identificador — o qual é usado para autenticar positivamente um solicitante —, eles poderão tratá-lo com mais respeito.

Nenhuma empresa — bem, pelo menos muito poucas — dá os números dos telefones diretos de seus CEOs ou diretores. A maioria das empresas, porém, não se preocupa em dar os números de telefones da maioria dos departamentos e grupos de trabalho da organização — particularmente para alguém que é ou parece ser um empregado. Uma medida de contra-ataque possível seria implementar uma política que proíbe a divulgação dos números internos de funcionários, contratados, consultores e temporários para as pessoas que não são da empresa. O mais importante é desenvolver um procedimento passo a passo para identificar positivamente se um interlocutor que está pedindo os números de telefone é de fato um empregado.

Recado do Mitnick

Como diz o ditado; até mesmo os verdadeiros paranóicos provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus — os atacantes que visam a infra-estrutura da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados.

- Os códigos contábeis dos grupos de trabalho e departamentos, bem como as cópias do diretório corporativo (uma cópia impressa, um arquivo de dados ou uma lista eletrônica de telefones na intranet) são alvos freqüentes dos engenheiros sociais. Cada empresa precisa ter uma política escrita e bem divulgada sobre a revelação desse tipo de informação. As salvaguardas

devem incluir a manutenção de um registro de auditoria que estabelece os casos em que as informações sigilosas são divulgadas para as pessoas de fora da empresa.

- Informações, tais como um número de empregado, por si só, não devem ser usadas como nenhum tipo de autenticação. Todo empregado deve ser treinado para verificar não apenas a identidade do solicitante, como também a necessidade que o requisitante tem de saber
- No seu treinamento de segurança, você deve pensar em ensinar essa abordagem aos funcionários: sempre que um estranho pedir um favor, saiba primeiro como negar educadamente até que a solicitação possa ser verificada. Em seguida, antes de ceder ao desejo natural de ser o Sr ou a Sra. Ajuda, siga as políticas e os procedimentos da empresa com relação a verificação e divulgação das informações não públicas. Esse estilo pode ir contra a nossa tendência natural de ajudar os outros, mas um pouco de paranóia saudável pode ser necessária para evitar ser a próxima vítima do engenheiro social.

Como mostraram as histórias deste capítulo, as informações aparentemente inofensivas podem ser a chave para os segredos mais valiosos da sua empresa.

Capítulo 3

O Ataque Direto: Simplesmente Pedindo

Muitos ataques de engenharia social são complicados e envolvem diversas etapas e planejamento elaborado, além de combinar o conhecimento da manipulação e tecnologia.

Sempre achei incrível como um engenheiro social habilidoso pode atingir esse objetivo com um ataque simples e direto. Como você verá, às vezes tudo o que ele precisa é simplesmente pedir as informações.

UM MLAC RÁPIDO

Você quer saber o telefone de alguém que não está na lista? Um engenheiro social pode lhe dar meia dúzia de maneiras (e você encontrará algumas delas descritas nas histórias deste livro), mas provavelmente o cenário mais simples é aquele que usa uma única ligação telefônica como esta, a seguir

O número, por favor

O atacante discou para o número particular da empresa de telefonia do MLAC, o Centro Mecanizado de Designação de Linhas. Uma mulher respondeu e ele disse:

"Olá, aqui e Paul Anthony. Eu sou um técnico de cabos. Ouça, uma caixa de terminal aqui foi queimada em um incêndio. Os policiais acham que algum maluco tentou queimar sua própria casa para receber o seguro. Eles me mandaram aqui sozinho para tentar refazer a fiação de todo este terminal de duzentos pares. Eu estou precisando de ajuda. Quais instalações deveriam estar funcionando na South Main, 6723?".

Em outras empresas de telefonia, a pessoa chamada deveria saber que as informações de pesquisa inversa sobre os números não publicados devem ser fornecidas apenas para o pessoal autorizado da própria empresa de telefonia. Mas o MLAC só é conhecido dos empregados da empresa de telefonia. E embora eles nunca deêm informações para o público, quem iria se recusar a ajudar um homem da empresa que está tentando dar conta de uma tarefa difícil? Ela lamentou o fato, porque ela mesma já havia tido dias ruins no trabalho e poderia quebrar um pouco as regras para ajudar um colega com problemas. Ela forneceu o cabo, os pares e cada número em funcionamento designado para aquele endereço.

Analisando a trapaça

Como você vai notar em todas essas histórias, o conhecimento da linguagem de uma empresa e de sua estrutura corporativa — seus vários escritórios e departamentos, o que cada um deles faz e as informações que tem — faz parte da bagagem essencial de truques de um engenheiro social bem-sucedido.

Recado do Mitnick

É da natureza humana confiar em nossos colegas, particularmente quando a solicitação passa no teste como sendo razoável. Os engenheiros sociais usam esse conhecimento para explorar suas vitimas e atingir seus objetivos.

UM JOVEM EM FUGA

Um homem que chamaremos de Frank Parsons estava foragido há anos, e ainda era procurado pelo governo federal por fazer parte de um grupo antiguerra nos anos de 1960. Nos restaurantes, ele se sentava de frente para a porta e tinha um jeito desconcertante de sempre estar olhando para trás. Ele se mudava de tempos em tempos.

Certa vez Frank chegou em uma cidade que não conhecia e começou a procurar emprego. Para alguém como Frank, com as suas habilidades bem desenvolvidas com computadores (e também com habilidades de engenharia social, embora ele nunca tenha relacionado isso em uma proposta de emprego), encontrar um bom trabalho em geral não era problema. Exceto nas épocas em que a economia estava muito difícil, o talento das pessoas com um bom conhecimento técnico de computadores estava em alta e elas não tinham muitos problemas para dar um jeito. Frank rapidamente encontrou uma oportunidade de emprego com um bom salário em uma empresa grande perto de onde ele estava morando.

Isso é perfeito, pensou. Mas quando começou a preencher os formulários para o emprego, encontrou um empecilho: o empregador exigia que o candidato fornecesse uma cópia da sua ficha criminal, a qual ele teria de obter na polícia estadual. A pilha de documentos do emprego incluía um formulário para solicitar esse documento, e o formulário tinha um quadradinho para uma impressão digital. Embora eles estivessem pedindo uma digital apenas do indicador direito, se eles a comparassem com uma do banco de dados do FBI, ele provavelmente em breve estaria trabalhando na cozinha de um resort financiado pelo governo federal.

Ocorreu a Frank que talvez, apenas talvez, ele ainda pudesse contornar esse problema. Talvez o estado não enviasse aquelas amostras de digitais para o FBI. Como descobriria isso?

Como? Ele era um engenheiro social — como você *acha* que ele descobriu? Ele fez uma ligação telefônica para a polícia estadual: "Olá. Estamos fazendo um estudo para o Departamento de Justiça do Estado. Estamos pesquisando os requisitos para implementar um novo sistema de identificação de digitais. Posso falar com alguém que conheça aquilo que estamos fazendo e que possa nos ajudar?"

Quando o especialista local veio ao telefone, Frank fez uma série de perguntas sobre quais sistemas eles usavam e as capacidades de pesquisa e armazenamento de dados das digitais. Eles haviam tido algum problema com o equipamento? Eles estavam ligados à Pesquisa de Digitais do Centro Nacional de Informações sobre o Crime (NCIC) ou a jurisdição era apenas dentro do estado? O equipamento era fácil e todos poderiam aprender a usar?

Astuciosamente, ele incluiu a pergunta-chave entre as outras.

A resposta soou como música para seus ouvidos: não, eles não estavam ligados ao NCIC, eles verificavam apenas no índice de Informações Criminais (CII).

Recado do Mitnick

Os trapaceiros de informações experientes não têm escrúpulos em ligar para os governos federal, estadual ou municipal para saber os procedimentos da aplicação das leis. Com tais informações em mãos, o engenheiro social pode contornar as verificações de segurança padrão da sua empresa.

Isso era tudo que Frank precisava saber Ele não linha nenhum registro naquele estado, de modo que enviou o pedido de emprego, foi contratado e ninguém jamais apareceu na sua mesa um dia com esta conversa "Estes senhores são do FBI e gostariam de conversar com você".

DEIXE NA PORTA

Apesar do mito do escritório sem papelada, as empresas continuam imprimindo uma quantidade imensa de papel todos os dias. As informações impressas da sua empresa podem ser vulneráveis, mesmo que você use as precauções de segurança e coloque um carimbo de confidencial

Esta é uma história que mostra como os engenheiros sociais podem obter os seus documentos mais secretos.

A trapaça do loop-around

Todos os anos a empresa de telefonia publica uma lista chamada Lista de Números de Teste (ou pelo menos costumavam fazer isso, mas como eu ainda estou na condicional não vou perguntar se ainda a publicam). Esse documento era muito cobiçado pelos phreakers porque ele trazia uma lista de todos os números de telefone guardados a sete chaves e usados pelos funcionários, técnicos e outros empregados da empresa de telefonia para coisas como teste de tronco ou verificação de números que sempre estão ocupados.

Um desses números de teste, conhecido pelo jargão de *loop-around*, era particularmente útil. Os phreakers o usavam como um modo de entrar em contato com outros phreakers para conversar sem pagar pela ligação. Também costumavam usá-lo como um modo de criar um número de retorno para dar, por exemplo, a um banco. Um engenheiro social diria a alguém do banco o número de telefone do seu escritório? É claro que não. Quando o banco ligava de volta para o número de teste (loop-around), o phreaker podia receber a ligação, mas tinha a proteção de usar um número que não poderia ser rastreado e ele não seria encontrado.

Uma Lista de Números de Teste fornecia muitas informações boas que poderiam ser usadas por qualquer phreaker faminto por informações. Assim sendo, quando as novas listas eram publicadas todos os anos, elas eram cobiçadas por muitas crianças cujo hobby era explorar a rede de telefonia.

O golpe de Stevie

É claro que as empresas de telefonia não deixam que essas listas sejam conseguidas facilmente e os phreakers têm de ser criativos para conseguir uma. Como eles podem fazer isso? Uma criança ansiosa com uma mente determinada a conseguir a lista poderia criar um cenário como este.

Recado do
Mitnick

O treinamento de segurança com relação à política da empresa criada para proteger o ativo de informações precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao ativo de IT da empresa.

Em certa noite de outono no sudeste da Califórnia, Stevie liga para o escritório central pequeno da empresa de telefonia, estabelecido no prédio no qual as linhas telefônicas vão para todas as residências e empresas da área de serviço estabelecida.

Quando a telefonista de plantão atende, Stevie anuncia que trabalha na divisão da empresa de telefonia que publica e distribui o material impresso. "Temos a nossa nova Lista de Números de Teste", explica. "Mas por questões de segurança não podemos lhe entregar uma cópia antes de retirarmos a antiga. E o cara da entrega está atrasado. Se você puder deixar a sua cópia do lado de fora da porta, ele pode passar por aí, pegar a sua cópia, deixar a cópia nova e continuar o seu caminho."

O desavisado telefonista parece achar que isso é razoável. Ele faz exatamente o que foi pedido, coloca na porta do prédio a sua cópia da lista, a qual tem na capa um aviso em grandes letras verme lhas **"CONFIDENCIAL DA EMPRESA** --- QUANDO NÃO FOR MAIS NECESSÁRIO, ESTE DOCUMENTO DEVE SER DESTRUÍDO".

Stevie estaciona o carro e olha em volta para saber se há policiais ou o pessoal da segurança da empresa de telefonia espreitando atrás das árvores ou observando em carros estacionados. Ninguém á vista. Ele pega calmamente a cobiçada lista e vai embora.

Este é apenas mais um exemplo de como é fácil para um engenheiro social conseguir o que quer seguindo o princípio simples de "apenas pedir".

ATAQUE DE GÁS

Em um cenário da engenharia social, os ativos da empresa não são os únicos que correm riscos. Às vezes, as vítimas são os clientes de uma empresa.

O trabalho no serviço ao cliente tem a sua parcela de frustração, a sua parcela de risadas e a sua parcela de erros inocentes — sendo que alguns deles podem ter conseqüências infelizes para os clientes de uma empresa.

A história de Janie Acton

Janie Acton era atendente do serviço ao cliente da Hometown Electric Power, em Washington, D.C., há pouco mais de três anos. Ela era considerada como uma das melhores atendentes, inteligente e consciencioso.

Era a semana de Ação de Graças quando esta ligação foi recebida. O interlocutor disse: "Aqui é Eduardo do Departamento de Faturamento. Tenho uma senhora na linha, ela é uma secretária do escritório executivo e trabalha para um dos vice-presidentes, Ela está pedindo algumas informações e

não posso usar o meu computador. Recebi um e-mail de uma garota de Recursos Humanos que dizia **"ILOVEYOU"** e quando abri o anexo, não consegui mais usar a minha máquina. Um vírus. Fui pego por um vírus estúpido. De qualquer forma, você poderia procurar algumas informações de cliente para mim?"

"E claro", Janie respondeu. "Ele destruiu o seu computador? Isso é terrível."

'Sim."

'Como posso ajudar?", Janie perguntou.

Nesse ponto o atacante recorreu às informações da sua pesquisa avançada para parecer mais autêntico. Ele descobriu que as informações que queria estavam armazenadas em algo chamado Sistema de Informações de Faturamento do Cliente e descobriu como os empregados se referiam ao sistema. Ele perguntou: "Você pode abrir uma conta do CBIS?"

"Sim, qual é o número da conta?"

"Não tenho o número, preciso que você a abra pelo nome."

"Muito bem, qual é o nome?"

"O nome é Heather Marning". Ele soletrou o nome e Janie o digitou.

"Aqui está."

"Ótimo, a conta está atualizada?"

"Hum, hum, está sim."

"Qual é o número da conta?", ele perguntou.

"Você tem um lápis?"

"Pronto para anotar."

"Número de conta BAZ6573NR27Q."

Ele releu o número e, em seguida, acrescentou: "E qual é o endereço de serviço?"

Ela lhe deu o endereço.

"E qual e o telefone?"

Janie gentilmente leu essa informação também.

O interlocutor agradeceu, disse adeus e desligou. Janie foi para a próxima ligação e nunca mais pensou nisso.

O projeto de pesquisa de Art Sealy

Art Sealy desistiu de trabalhar como editor free lance para pequenas editoras quando descobriu que poderia ganhar mais dinheiro realizando pesquisa para autores e empresas. Ele descobriu que a taxa que poderia cobrar aumentava na proporção em que a tarefa o levava mais perto da linha às vezes indistinta entre o que é legal e o que é ilegal. Sem nunca perceber e certamente sem nunca lhe dar este nome, Art tornou-se um engenheiro social e usava as técnicas que são conhecidas de todo corretor de informações. Ele descobriu que tinha um talento nato para isso e aprendeu sozinho as técnicas que a maioria dos engenheiros sociais tinha de aprender com os outros. Após algum tempo, ele cruzou a linha sem o mínimo resquício de culpa.

Um homem entrou em contato comigo. Ele estava escrevendo um livro sobre o Gabinete do governo Nixon e procurava um pesquisador que pudesse investigar William E. Simon, que havia sido o secretário do Tesouro de Nixon. O Sr. Simon havia morrido, mas o autor tinha o nome de uma mulher que havia pertencido à sua equipe. Ele estava certo de que ela ainda morava em D.C, mas não conseguira encontrar o seu endereço. Ela não tinha um telefone em seu nome, ou pelo menos seu nome não estava na lista. Assim sendo, eles me ligaram. Eu disse a ele que não teria problema.

Esse é o tipo de trabalho que geralmente você realiza em uma ou duas ligações telefônicas, se souber o que está fazendo. Toda empresa telefônica local pode dar as informações. Obviamente, você tem de mentir um pouco. Mas uma mentirinha de vez em quando não faz mal a ninguém, certo?

Gosto de usar uma abordagem diferente de cada vez. só para que as coisas fiquem interessantes. "Este *é* fulano do escritório executivo" sempre funcionou para mim. Assim como "tenho alguém na linha do escritório do vice-presidente Fulano", que também funcionou desta vez.

Recado do Mitnick

Nunca ache que os ataques da engenharia social precisem ter mentiras elaboradas tão complexas que provavelmente serão reconhecidas antes de serem concluídas. Alguns são ataques diretos, rápidos e muito simples, os quais nada mais são do que... bem. simplesmente pedir as informações.

Você tem de desenvolver o instinto do engenheiro social, precisa ter uma idéia da disposição da pessoa que está do outro lado em cooperar com você. Desta vez tive a sorte de encontrar uma senhora amistosa e útil Em uma única ligação telefônica consegui o endereço e o número de telefone. Missão cumprida.

Analisando a trapaça

Certamente Janie sabia que as informações de clientes são sigilosas. Ela nunca discutiria a conta de um cliente com outro cliente, nem daria informações particulares para o público.

Mas é claro que para um interlocutor de dentro da empresa as regras são diferentes. Para um colega de trabalho tudo se reduz a fazer parte da equipe e ajudar um ao outro a fazer o trabalho. O homem do Departamento de Faturamento poderia ter ele mesmo procurado os detalhes se o seu computador não tivesse sofrido um ataque de vírus, e ela ficou contente em poder ajudar um colega.

O atacante chegou aos poucos às informações principais que desejava fazendo perguntas sobre coisas que não queria saber, tais como o número da conta. Mesmo assim, o número de conta forneceu uma segurança a mais. Se o atendente suspeitasse, ele ligaria uma segunda vez e teria mais chances de sucesso, porque o conhecimento do número de conta faria com que ele parecesse mais autêntico para o atendente que ele ligasse.

Nunca ocorreu a Janie que alguém pudesse mentir sobre algo assim, que o interlocutor pudesse não estar no Departamento de Faturamento, E claro que a culpa não é de Janie. Ela não dominava bem a regra sobre ter certeza de que você sabe com quem está falando antes de discutir as informações do arquivo de um cliente. Ninguém jamais disse a ela sobre o perigo de uma ligação telefônica como essa que ela recebeu, Isso não estava na política da empresa, não fazia parte do seu treinamento e o seu supervisor nunca mencionou algo semelhante.

EVITANDO A TRAPAÇA

Um ponto a ser incluído no seu treinamento de segurança: só porque um interlocutor ou visitante conhece os nomes de algumas pessoas da empresa ou conhece alguns jargões ou procedimentos corporativos, isso não quer dizer que ele *é* quem alega ser E isso definitivamente não o estabelece como alguém que está autorizado a receber informações internas, nem acessar o seu sistema ou rede de computadores.

O treinamento em segurança precisa enfatizar que quando estiver em dúvida, você precisa verificar, verificar e verificar,

Nos tempos antigos, o acesso às informações dentro de uma empresa era uma marca de prestígio e privilégio. Os empregados abasteciam os fornos, faziam as máquinas funcionar, datilografavam as cartas *e* preenchiam relatórios. O encarregado ou chefe lhes dizia o que fazer, quando e como. Era o encarregado ou chefe que sabia quantos parafusos cada empregado deveria produzir em cada turno, o número, as cores e os tamanhos que a fábrica precisava produzir nesta semana, na próxima e no final do mês.

Os empregados lidavam com as máquinas, ferramentas e materiais e os chefes lidavam com as informações. Os empregados só precisavam saber das informações que eram específicas de suas funções.

O quadro hoje é um pouco diferente, não é? Muitos trabalhadores em fábricas usam computadores ou máquinas computadorizadas. Para uma grande parte da força de trabalho, as informações críticas são colocadas nos desktops dos usuários para que eles possam cumprir a sua responsabilidade e fazer seu trabalho. No ambiente de hoje, quase tudo o que os empregados fazem envolve o tratamento das informações.

Por esse motivo a política de segurança de uma empresa precisa ser estendida a toda a empresa, independentemente da posição. Todos devem entender que não são apenas os executivos e os chefes que tem as informações que um atacante pode estar procurando. Hoje em dia, os empregados de todos os níveis, até mesmo aqueles que não usam um computador, podem ser os alvos. O representante recém-contratado do grupo de serviço ao cliente pode ser o elo mais fraco que um engenheiro social quebra para atingir o seu objetivo.

O treinamento em segurança e as políticas corporativas de segurança precisam fortalecer esse elo.

Capítulo 4

Criando a Confiança

Algumas dessas histórias podem levá-lo a imaginar que acredito que todas as pessoas que estão nos negócios são completas idiotas, prontas e até mesmo ansiosas para revelar cada um dos segredos que possuem. O engenheiro social sabe que isso não é verdade. Por que os ataques da engenharia social são tão bem-sucedidos? isso não acontece porque as pessoas são estúpidas ou não têm bom senso, Mas nós. como seres humanos, somos todos sujeitos a ser enganados, porque a confiança das pessoas pode ser usada de forma errada se for manipulada de determinadas maneiras.

O engenheiro social prevê a suspeita e a resistência, e ele está sempre preparado para transformar a desconfiança em confiança. Um bom engenheiro social planeja o seu ataque como um jogo de xadrez, e prevê as perguntas que o seu alvo pode fazer para estar pronto para dar as respostas corretas.

Uma dessas técnicas comuns envolve a criação de uma sensação de confiança por parte da sua vítima. Como um trapaceiro pode fazer com que você confie nele? Confie em mim, ele pode.

CONFIANÇA: O SEGREDO DA FRAUDE

Quanto mais os engenheiros sociais puderem dar a aparência de negócios normais ao seu contato, menos eles levantam suspeitas. Quando as pessoas não têm um motivo para suspeitar, um engenheiro social pode ganhar 3 sua confiança mais facilmente.

Após conseguir a sua confiança, a ponte levadiça e abaixada e o portão do castelo se abre para que ele entre e obtenha as informações desejadas.

Observação

Você já deve ter notado que me refiro aos engenheiros sociais, phreakers e operadores do jogo da trapaça como "ele" na maioria das histórias. Isso não é chauvinismo, mas apenas reflete a realidade de que a maioria dos praticantes dessa área é masculina, Mas embora não existam muitas engenheiras sociais, esse número está crescendo. Há engenheiras sociais suficientes para que você não baixe a guarda só porque está ouvindo uma voz feminina. Na verdade, as engenheiras sociais têm uma vantagem distinta porque podem usar a sua sensualidade para obter a cooperação. Você encontrará alguns poucos exemplos do chamado sexo frágil representado nestas páginas.

A primeira ligação: Andrea Lopez

Andrea Lopez atendeu ao telefone na locadora de vídeo na qual trabalhava, e em instantes estava sorrindo: "É sempre um prazer quando um cliente se dá ao trabalho de dizer que está satisfeito com o nosso serviço." Esse interlocutor disse que teve uma experiência muito boa ao ser atendido pela loja e queria enviar uma carta para o gerente dizendo isso.

Ele pediu o nome e endereço de correspondência do gerente, e ela disse que seu nome era Tommy Allison e deu o endereço. Quando ela estava para desligar, ele teve outra idéia e pediu: "Eu poderia escrever para a sede da sua empresa também. Qual é o número da sua loja?" Ela forneceu essas informações também. Ele agradeceu, acrescentou algo agradável sobre como ela ajudou e disse adeus.

Ela pensou: "Uma ligação assim sempre parece melhorar o nosso dia de trabalho. Que bom se as pessoas fizessem isso com mais freqüência."

A segunda ligação: Ginny

"Obrigada por ligar para a Studio Video. Meu nome é Ginny, posso ajudar?"

"Oi, Ginny", disse o interlocutor com voz entusiasmada, como se ele falasse com Ginny todas as semanas. "Aqui é Tommy Allison, gerente da Loja 863, Forest Park. Temos um cliente aqui que quer alugar *Rocky* 5 e estamos sem nenhuma cópia. Você pode verificar se vocês têm uma?"

Após alguns momentos ela voltou ao telefone e confirmou: "Sim, temos três cópias."

"Muito bem. Vou ver se ele quer passar aí. Olha, obrigado. Se precisar de alguma ajuda da nossa loja. é só ligar e pedir para falar com Tommy. Vou ficar feliz em ajudar como puder."

Três ou quatro vezes nas próximas semanas Ginny recebeu ligações de Tommy pedindo ajuda com uma ou outra coisa. As solicitações aparentemente eram legítimas e ele sempre era tão amistoso, sem parecer que estava tentando se aproveitar disso. Ele começou a bater papo também — "Você ouviu falar do grande incêndio em Oak Park? Várias ruas foram fechadas" e outras coisas do gênero. As ligações quebravam um pouco a rotina do dia e Ginny sempre gostava de ouvi-lo.

Certo dia Tommy ligou e parecia meio estressado. Ele perguntou: Vocês estão tendo problemas com seus computadores?"

"Não". Ginny respondeu. "Por quê?"

"Alguém bateu o carro contra um telefone público e o pessoal da empresa de telefonia disse que grande parte da cidade vai perder seus telefones e conexão com a Internet até eles resolverem o problema."

"Ah, não. O homem se machucou?"

"Eles o levaram em uma ambulância. De qualquer maneira, você poderia me ajudar? Tenho um cliente seu aqui que queria alugar *O poderoso chefão II* e está sem o cartão. Você poderia verificar essas informações para mim?"

"Sim, é claro."

Tommy deu o nome e endereço do cliente e Ginny o encontrou no computador, Ela deu a Tommy o número da conta.

"Ele tem alguma devolução a fazer ou saldo devedor?", Tommy perguntou.

"Não consta nada."

"Multo bem, ótimo. Vou abrir uma conta para ele aqui à mão e o coloco no nosso banco de dados mais tarde quando os computadores voltarem a funcionar. Ele quer pagar com o cartão Visa que ele usa na sua loja e também está sem ele. Qual é o número do seu cartão e a data de vencimento?"

Ela também forneceu essas informações. Tommy agradeceu: "Olha, obrigado pela ajuda. Falo com você depois", e desligou.

A história de Doyle Lonnegan

Lonnegan não é um jovem que você gostaria de encontrar ao abrir a sua porta. Ele é um cobrador de dividas em atraso e ainda presta favores eventuais, se isso não o atrapalhar muito. Neste caso, ele recebeu uma quantia razoável em dinheiro para apenas fazer algumas ligações telefônicas para uma locadora de vídeo. Isso parece fácil. So que nenhum de seus "clientes" sabia como executar esse golpe; eles precisavam de alguém com o talento e *know-how* de Lonnegan.

As pessoas não preenchem cheques para pagar suas apostas quando não têm sorte ou fazem alguma besteira na mesa de pôquer Todos sabem disso. Por que esses meus amigos continuam apostando em algo que não pode dar certo? Não me pergunte. Talvez eles estejam um pouco em desvantagem no departamento de QI. Mas eles são meus amigos, o que se pode fazer?

Esse homem não tinha o dinheiro e eles aceitaram um cheque. Pergunto: eles não deveriam tê-lo levado a um caixa eletrônico? E isso o que eles deveriam ter feito. Mas não, eles aceitaram um cheque de US$ 3.230,00. Naturalmente o cheque voltou. O que você esperaria? Aí eles me ligam, posso ajudar? Não fecho mais as portas quando as pessoas batem. Além disso, hoje em dia há maneiras melhores de fazer isso. Contei-lhes que queria comissão de 30%, e veria o que podia fazer. Assim sendo, eles me deram seu nome e endereço e procurei no computador qual era a locadora de vídeo mais próxima dele.

Não estava com muito pressa. Quatro ligações telefônicas para nos deixar mais próximos do gerente da loja e bingo, eu havia conseguido o número do cartão Visa do homem. Outro amigo meu tem um bar de topless. Por cinqüenta pratas ele colocou o dinheiro do pôquer dessa pessoa como uma conta no cartão Visa feita no bar. Vamos ver como o escroque vai explicar isso para a sua mulher. Você acha que tentaria dizer à administradora do Visa que a conta não *é* sua? Pense de novo. Ele sabe que sabemos quem ele é. E se conseguimos o seu número do cartão Visa, ele vai imaginar que podemos descobrir muito mais. Caso encerrado.

Analisando a trapaça

As ligações iniciais de Tommy para Ginny visavam apenas criar confiança. Quando chegou a hora do ataque real, ela baixou a guarda e aceitou que Tommy era quem alegava ser, o gerente de outra loja do grupo.

E por que *não o aceitaria*[1]*?* Ela já o conhecia. Ela só o conhecia por telefone, mas eles haviam estabelecido uma amizade comercial que é a base da confiança. Depois de aceitá-lo como autoridade, como um gerente da mesma empresa, a confiança havia sido estabelecida e o resto era fácil.

Recado do Mitnick

Essa técnica para criar a confiança é uma das mais eficientes da engenharia social. Você tem de pensar se realmente conhece a pessoa com quem está falando. Em alguns raros casos, a pessoa talvez não possa ser quem alega ser. Da mesma forma, todos temos de aprender a observar, pensar e questionar a autoridade.

VARIAÇÃO SOBRE UM MESMO TEMA: A CAPTURA DO CARTÃO

A criação de uma sensação de confiança não exige necessariamente uma série de ligações telefônicas com a vítima, como sugere a história anterior. Lembro-me de um incidente que presenciei no qual foram necessários apenas cinco minutos.

Surpresa, papai!

Certa vez eu estava em um restaurante com Henry e seu pai. Durante a conversa, Henry repreendeu o pai por dar o número do seu cartão de crédito como quem dá o número do telefone. "É claro que você tem de dar o número do seu cartão quando compra alguma coisa", ele dizia. "Mas dá-lo em uma loja que arquiva o seu número em seus registros — isso é burrice."

"O único lugar em que faço isso é na Studio Video", disse o Sr Conklin, referindo-se à mesma cadeia de locadoras de vídeo. "Mas verifico a minha fatura todos os meses. Eu percebo se eles começarem a aumentar a conta."

"É claro", salientou Henry, "mas depois que eles têm o seu número, qualquer pessoa pode roubá-lo".

"Você se refere a um funcionário desonesto?"

"Não, *qualquer pessoa* e não apenas um funcionário."

"Você está dizendo bobagens", retrucou o Sr. Conklin.

"Posso ligar agora mesmo e fazer com que eles me dêem o número do seu cartão Visa", respondeu Henry.

"Não, você *não pode"*, afirmou o pai.

"Posso fazer isso em cinco minutos, bem na sua frente sem nem ter de sair da mesa."

O Sr. Conklin olhou firme, o olhar de alguém que se sentia seguro, mas que não queria mostrar isso. "Digo que você não sabe do que está falando", desafiou, tirando do bolso a carteira e jogando uma nota de 50 dólares na mesa. "Se fizer o que está dizendo, o dinheiro é seu."

"Não quero o seu dinheiro pai", disse Henry.

Ele pegou o telefone celular, perguntou ao pai qual era a loja e ligou para o Auxílio à Lista pedindo o número do telefone e também o número da loja na região de Sherman Oaks.

Em seguida, ligou para a loja de Sherman Oaks. Usando mais ou menos a mesma abordagem descrita na história anterior, ele rapidamente conseguiu o nome do gerente e o número da loja.

Ligou para a loja na qual o seu pai tinha a conta. Ele usou o velho truque de se fazer passar pelo gerente, deu o nome do gerente como o seu próprio e o número da loja que havia obtido. Tomou a

usar o mesmo truque: "Os seus computadores estão funcionando hoje? Os nossos às vezes funcionam, às vezes não." Ouviu a resposta e continuou: "Bem, tenho um dos seus clientes aqui comigo e ele quer alugar um vídeo, mas os nossos computadores estão fora do ar agora. Preciso ver a conta do cliente e ter certeza de que ele é um cliente da sua loja."

Henry deu o nome do seu pai. Em seguida, usando apenas uma pequena variação da técnica, pediu para ela ler as informações da conta: endereço, número de telefone e a data em que a conta foi aberta. Depois disse: "Ouça, estou com uma fila enorme de clientes aqui. Qual é o número do cartão de crédito e a data de vencimento?"

Henry segurou o celular no ouvido com uma mão e com a outra escreveu em um guardanapo de papel. Ao terminar a ligação, ele colocou o guardanapo na frente do pai, que ficou olhando para o número de boca aberta. O pobre senhor parecia totalmente chocado, como se todo o seu sistema de confiança tivesse ido por água abaixo.

Analisando a trapaça

Pense na sua própria atitude quando alguém que você não conhece pede alguma coisa. Se um pobre bate à sua porta, você provavelmente não o deixa entrar; se um estranho bem vestido bater à porta, de sapatos brilhantes, cabelo bem penteado, bons modos e um sorriso, você provavelmente terá menos suspeitas. Talvez ele seja o Jason do filme *Sexta-Feira 13,* mas você está disposto a confiar naquela pessoa, desde que ela tenha uma aparência normal e não tenha uma faca na mão.

Á questão menos óbvia é que julgamos as pessoas da mesma forma pelo telefone. Essa pessoa dá a impressão de estar tentando me vender alguma coisa? Ele é amistoso e aberto ou sinto algum tipo de hostilidade ou pressão? Ele tem o discurso adequado para uma pessoa educada? Julgamos essas coisas e talvez mais uma dezena de outras inconscientemente em um relance, quase sempre nos primeiros momentos da conversação.

Recado do Mitnick

É da natureza humana achar que é improvável que você seja enganado em determinada transação, pelo menos até que tenha algum motivo para acreditar no contrário, Nós ponderamos o risco e, em seguida, na maior parte das vezes, damos às pessoas o benefício da dúvida. Esse é o comportamento natural das pessoas civilizadas... pelo menos as pessoas civilizadas que nunca foram enganadas, manipuladas ou trapaceadas em uma soma grande em dinheiro. Quando éramos crianças, nossos pais nos ensinavam a não confiar em estranhos. Talvez todos devêssemos adotar esse antigo princípio no ambiente de trabalho de hoje.

No trabalho, as pessoas nos solicitam coisas o tempo todo. Você tem o endereço de e-mail desta pessoa? Onde está a última versão da lista de clientes? Quem é o subcontratado desta parte do projeto? Por favor, me envie a atualização mais recente do projeto. Preciso da versão nova do código-fonte.

E adivinhe o que acontece? Às vezes as pessoas que fazem essas solicitações são aqueles que você não conhece pessoalmente, gente que trabalha em outra parte da empresa ou que alega trabalhar. Mas se as informações que dão coincidem e parecem ter o conhecimento ("Marianne disse...", "Isso

está no servidor K-16...."; "...a revisão 26 dos planos do novo produto"), estendemos o nosso círculo de confiança para inclui-los e alegremente fornecemos aquilo que estão pedindo.

Certamente devemos parar um pouco e nos perguntar. "Por que alguém na fábrica de Dallas precisa ver os planos do produto novo?" ou "Será que você podia me dar o nome do servidor no qual ele está?". Assim, fazemos outras perguntas. Se as respostas parecem razoáveis e a maneira como a pessoa responde é segura, baixamos a guarda, voltamos a nossa inclinação natural de confiar no nosso colega e fazemos (com toda a razão) tudo que ele quer que façamos.

E não pense nem por um momento que o atacante só visa as pessoas que usam os sistemas de computadores da empresa, Que tal o cara da sala de correspondência? "Você me faz um favor? Coloque isto no malote interno?". O funcionário da sala de correspondência sabe que o envelope contém um disquete com um programa especial para a secretária do CEO? Agora aquele atacante tem a sua própria cópia pessoal do e-mail do CEO. Ufa! Isso pode acontecer na sua empresa? É claro que pode.

O TELEFONE CELULAR DE UM CENTAVO

Muitas pessoas procuram até achar um bom negócio. Os engenheiros sociais não procuram um bom negócio, eles encontram um modo de transformar algo em um bom negócio. Por exemplo, às vezes uma empresa lança uma campanha de marketing que é tão boa que você não consegue deixar de aproveitá-la, enquanto o engenheiro social olha a oferta e pensa em como ele pode melhorá-la.

1 lá pouco tempo, uma empresa nacional de telefonia sem fio fez uma grande promoção oferecendo um telefone novo por um centavo quando você se inscrevia em um dos seus planos de chamada.

Como muitas pessoas acabaram descobrindo tarde demais, existem boas perguntas que um comprador prudente deve fazer antes de se inscrever em um plano de chamadas de telefone celular — se o serviço é analógico, digital ou uma combinação entre eles; o número de minutos que podem ser usados no mês; se as taxas de roaming estão incluídas... e assim por diante. E importante entender desde o início qual é o prazo de comprometimento do contrato — por quantos meses ou anos você ficará comprometido?

Pense em um engenheiro social da Filadélfia que é atraído por um modelo de telefone barato oferecido por uma empresa de telefonia celular mediante uma inscrição, mas ele odeia o plano de chamada que acompanha o aparelho. Tudo bem. Aqui está como ele trataria dessa situação.

A primeira ligação: Ted

Em primeiro lugar, o engenheiro social liga para uma cadeia de produtos eletrônicos em West Girard.

"Electron City, Ted."

"Oi. Ted. Aqui é Adam. Ouça. há algumas noites eu estava conversando com um vendedor sobre um telefone celular. Eu disse que ligaria de volta quando tivesse resolvido qual plano queria e esqueci o nome dele. Quem é a pessoa que trabalha no departamento no turno da noite?

"Há mais de um. Será que era o William?"

"Eu não tenho certeza. Talvez fosse o William. Como ele é?"

"Um homem alto e meio magro."

"Eu acho que era ele. Qual é mesmo o sobrenome dele?

"Hadley. H — A — D — L — E — Y."

"Isso, acho que é isso. Quando ele volta?"

"Não sei a sua escala para esta semana, mas o pessoal da noite chega em cinco minutos."

"Bom. Vou tentar falar com ele esta noite. Obrigado. Ted".

A segunda ligação: Katie

A próxima ligação é feita para uma loja da mesma cadeia na North Broad Street.

"Electron City. Aqui é Katie, posso ajudar?"

"Katie, olá. Aqui é William Hadley da loja da West Girard. Com vão as coisas?"

"Um pouco devagar, e aí?"

"Tenho um cliente que está interessado naquele programa do telefone celular por um centavo. Você sabe do que se trata?"

"Certo. Vendi alguns deles na última semana."

"Você ainda tem alguns dos telefones que acompanham aquele plano?"

"Tenho um monte deles."

"Ótimo, porque acabei de vender um para um cliente. O crédito desse cliente foi aprovado e ele assinou o contrato. Verifiquei o estoque e não temos nenhum telefone. Estou em uma situação complicada. Você pode me fazer um favor? Vou pedir para ele passar na sua loja e pegar um telefone. Você pode vender para ele o telefone de um centavo e dar-lhe um recibo? Ele deve me ligar de volta assim que pegar o telefone para eu ensinar como programar o aparelho."

"Sim, é claro. Mande ele aqui."

"OK. O nome dele é Ted. Ted Yancy."

Quando o homem que diz ser Ted Yancy aparece na loja da North Broad St., Katie faz uma fatura e vende para ele um telefone celular por um centavo, assim como o seu "colega" falou para ela fazer. Ela caiu feito um patinho.

Na hora de pagar, o cliente não tem moedas no bolso. Assim sendo, ele vai até o pratinho com moedas pequenas no balcão do caixa, pega uma e paga a garota da caixa registradora. Ele recebe o telefone sem ter pago nem um centavo por ele.

Ele está livre para ir até outra empresa de telefonia celular que usa o mesmo modelo de telefone e escolher qualquer plano de serviços que quiser. De preferência um plano mensal, sem nenhum comprometimento.

Analisando a trapaça

É natural que as pessoas tenham um grau alto de aceitação para com alguém que *diz* ser um colega do trabalho, e que conheça os procedimentos e a linguagem da empresa. O engenheiro social desta história aproveitou-se disso descobrindo os detalhes de uma promoção, identificando a si mesmo como empregado da empresa e pedindo um favor para outra filial. Isso acontece entre as filiais das lojas de varejo e entre os departamentos de uma empresa na qual as pessoas estão separadas fisicamente e lidam quase todos os dias com colegas de trabalho que nem conhecem.

UM GOLPE DE HACKER NOS FEDERAIS

Com freqüência, as pessoas não param para pensar no material que a sua organização está disponibilizando pela Web. Para o meu programa semanal na Rádio KF1 Talk, de Los Angeles, o produtor fez uma pesquisa *on-line* e descobriu uma cópia de um manual de instruções para acessar o banco de dados do Centro Nacional de Informações sobre o Crime. Mais tarde ele encontrou o próprio manual do NCIC *on-line,* um documento confidencial que dá todas as instruções para recuperar informações do banco de dados nacional de crimes do FBI.

O manual é um volume para os departamentos de polícia, o qual fornece a formatação e os códigos para recuperar as informações sobre os criminosos do banco de dados nacional. As agências de todo o país podem pesquisar o mesmo banco de dados para obter as informações que ajudam a solucionar os crimes de suas próprias jurisdições. O manual contém os códigos usados no banco de dados para designar tudo, desde os diferentes tipos de tatuagens, os diferentes cascos de barcos até as denominações de dinheiro e títulos roubados.

Todos que tenham acesso ao manual podem procurar a sintaxe e os comandos necessários para extrair as informações do banco de dados nacional. Em seguida, seguindo as instruções do guia de procedimentos e com um pouco de sangue frio, todos podem extrair as informações do banco de dados. O manual também fornece os números de telefone do suporte para obter as informações sobre como usar o sistema, Na sua empresa, você pode ter manuais semelhantes que oferecem códigos de produtos ou códigos para recuperar informações confidenciais.

O FBI com quase toda a certeza nunca descobriu que o seu manual e as instruções de procedimentos confidenciais estavam disponíveis para todas as pessoas *on-line,* e não acho que eles ficariam muito felizes se descobrissem. Uma cópia foi publicada por um departamento do governo no Oregon, a outra por um departamento de polícia no Texas. Por quê? Em cada um dos casos provavelmente alguém achou que as informações não tinham valor e que a sua publicação não causaria nenhum dano. Talvez alguém tenha publicado essas informações em sua intranet como uma conveniência para seus próprios empregados, e nunca tenha percebido que as informações estariam disponíveis para todos que estivessem na Internet com acesso a um bom mecanismo de pesquisa, tal como o Google — incluindo os simples curiosos, o pretendente a detetive, o hacker e o chefio do crime organizado.

Bisbilhotando o sistema

O princípio de usar tais informações para enganar alguém do governo ou de uma empresa privada é o mesmo. Como um engenheiro social sabe como acessar bancos de dados ou aplicativos específicos ou conhece os nomes dos servidores de computador de uma empresa ou coisa semelhante, ele tem credibilidade. E a credibilidade leva à confiança,

Depois que um engenheiro social tem tais códigos, a obtenção das informações de que precisa é um processo fácil. Neste exemplo, ele pode começar a ligar para um funcionário do escritório de teletipo da polícia estadual local e fazer perguntas sobre um dos códigos do manual — por exemplo, o código de agressão. Ele pode dizer algo como "Quando faço uma consulta OFF no NCIC, recebo um erro 'System is down' (Transação fora do ar). Você tem esse problema quando faz um OFF? Você poderia tentar para mim?". Ou quem sabe ele diria que estava tentando procurar um *wpf*— o jargão policial para o arquivo de uma pessoa procurada.

O funcionário do teletipo do outro lado do telefone entenderia a pista de que o interlocutor estava familiarizado com os procedimentos operacionais e os comandos para consultar o banco de dados do

NCIC. Quem mais além de alguém treinado no uso do NCIC conheceria esses procedimentos?

Após o funcionário confirmar que o sistema estava funcionando, a conversação poderia ter prosseguido mais ou menos assim:

"Você pode me ajudar?"

"O que você está procurando?"

"Preciso que você dê um comando OFF sobre Reardon, Martin. DOB 18/10/66."

"Qual é o sosh?" (As pessoas do departamento de polícia às vezes se referem ao número do seguro social como *sosh).*

"700-14-7435."

Após procurar na listagem, ela voltaria com algo do tipo "Ele tem um 2602".

O atacante só teria de olhar no NCIC *on-line* para descobrir o significado do número. O homem tem um caso de roubo em sua ficha.

Analisando a trapaça

Um engenheiro social experiente não pararia um minuto para pensar nas maneiras de invadir o banco de dados do NC1C. Por que ele faria isso, quando com uma simples ligação para o departamento local de policia e um pouco de conversa para mostrar que ele está por dentro, ele conseguiria o que quer? E da próxima vez ele apenas liga para um departamento diferente da polícia e usa o mesmo pretexto.

Recado do Mitnick

Todos devem ter conhecimento do *modus operandi* do engenheiro social, Ele coleta o máximo possível de informações sobre o alvo e usa essas informações para ganhar a confiança de alguém que trabalha dentro da empresa do alvo. Em seguida, ele ataca a jugular!

Você deve estar se perguntando se não é arriscado ligar para um departamento de polícia, o escritório de um delegado ou o escritório da guarda rodoviária. O atacante não corre um risco imenso?

A resposta é não... e por um motivo específico. As pessoas do departamento de polícia, assim como os militares, têm incutido nelas desde o seu primeiro dia na academia de polícia o respeito pela hierarquia, Desde que o engenheiro social esteja se fazendo passar por um sargento ou tenente — uma hierarquia mais alta do que aquela da pessoa com quem ele fala —, a vítima será governada pela lição bem aprendida que diz que você não questiona as pessoas com uma patente mais alta do que a sua.

Jargão

SOSH Gíria da polícia para o número do seguro social.

A patente. em outras palavras, tem seus privilégios, particularmente o privilégio de não ser desafiado pelas pessoas que estão abaixo na hierarquia.

Mas não pense que os policiais e os militares são os únicos que podem ter esse respeito pela hierarquia explorado pelo engenheiro social Eles quase sempre usam a autoridade ou patente da hierarquia corporativa como uma arma em seus ataques aos negócios — como demonstram várias das histórias deste livro.

EVITANDO A TRAPAÇA

Quais são algumas das etapas que a sua organização pode tomar para reduzir a probabilidade de que os engenheiros sociais aproveitem o instinto natural dos seus empregados de confiar nas pessoas? Estas são algumas sugestões.

Proteja os seus clientes

Nesta era eletrônica, muitas empresas que vendem para o consumidor mantém um arquivo de cartões de crédito. Existem motivos para isso: evitar que o cliente tenha de fornecer as informações do cartão de crédito sempre que visitar a loja ou o site na Web ou sempre que fizer uma compra. Entretanto. essa prática deve ser desencorajada.

Sc você precisar manter os números de cartões de crédito em um arquivo, esse processo tem de ser acompanhado por medidas de segurança que vão além da criptografia ou do controle de acesso. Os empregados precisam ser treinados para reconhecer os golpes da engenharia social semelhantes àqueles mostrados neste capitulo. Aquele colega de trabalho que você não conhece pessoalmente, mas que se tornou um amigo pelo telefone, talvez não seja quem ele alega ser. Ele pode não ter a "necessidade de saber" para acessar as informações confidenciais de cliente, porque ele pode não trabalhar na empresa.

Confie desconfiando

Não são apenas as pessoas que têm acesso a informações confidenciais — os engenheiros de software. o pessoal de P&D e assim por diante — que precisam se manter na defensiva contra as invasões. Quase todos da sua organização precisam de treinamento para protegerem a empresa contra os espiões industriais e os ladrões de informações.

A base disso deve começar com uma pesquisa das informações na empresa, um exame separado de cada ativo confidencial, crítico ou valioso e perguntas sobre quais métodos um atacante usaria para comprometer aqueles ativos por meio das táticas da engenharia social. O treinamento apropriado das pessoas que têm acesso de confiança a essas informações deve ser designado com base nas respostas para essas perguntas.

Quando alguém que você não conhece solicita informações ou materiais ou pede para executar uma tarefa no seu computador, os seus empregados fazem algumas perguntas do tipo: "Se dei essas informações para o meu pior inimigo, elas poderiam ser usadas para me prejudicar ou à minha empresa?" "Entendo o efeito em potencial dos comandos que estão pedindo para eu inserir no meu computador?"

Não queremos passar a vida toda suspeitando de cada nova pessoa que conhecemos. Mesmo assim, quanto mais confiamos, maiores as chances de que o próximo engenheiro social que chegar à cidade possa nos influenciar para dar informações da nossa empresa.

O que faz parte da sua Intranet?

Partes da sua intranet podem estar abertas para o mundo exterior e outras partes podem ser restritas aos empregados. Com que cuidado a sua empresa garante que as informações confidenciais não estão sendo publicadas em lugares onde estão acessíveis para públicos dos quais você quer protegê-las? Quando foi a última vez que alguém da sua organização verificou se alguma informação confidencial da intranet da sua empresa não foi acidentalmente disponibilizada por meio das áreas de acesso público do seu site na Web?

Se a sua empresa implementou servidores proxy como intermediários para proteger a empresa contra as ameaças eletrônicas à segurança, esses servidores foram verificados há pouco para saber se estão configurados adequadamente?

Na verdade, alguém alguma *vez* verificou a segurança da sua intranet?

Capítulo 5

"Posso Ajudar?"

Ficamos agradecidos quando lemos um problema e alguém com conhecimento, habilidade e disposição nos oferece ajuda. O engenheiro social entende isso e sabe como se aproveitar da situação.

Ele lambem sabe como *criar* um problema para você... para que depois você se sinta agradecido quando ele o solucionar... e finalmente joga com a sua gratidão para extrair algumas informações ou um pequeno favor que deixará a sua empresa (ou talvez você mesmo, como indivíduo) em um estado muito pior do que antes. E você talvez nunca saiba que perdeu algo de valor.

Estas são algumas maneiras típicas pelas quais os engenheiros sociais aparecem para "ajudar".

A QUEDA DA REDE

Dia/Hora: Segunda-feira, 12 de fevereiro, 15h25.

Local: Escritórios da Estaleiros Starboard

A primeira ligação: Tom DeLay

Tom DeLay, Contabilidade."

"Olá, Tom, aqui é Eddie Martin do Help Desk. Estamos tentando solucionar um problema de rede de um computador. Você sabe se alguém do seu grupo vêm tendo problemas para permanecer conectado?"

"Hum, não que eu saiba."

"E você não está tendo problemas?"

"Não, tudo parece bem."

"Bem, isso é bom. Ouça, estamos ligando para as pessoas que podem ser afetadas, por isso é Importante que você nos informe imediatamente se perder a sua conexão de rede."

"Isso não parece bom. Você acha que pode acontecer?"

"Esperamos que não, mas você liga se acontecer alguma coisa, certo?"

"Pode acreditar que sim."

"Ouça, parece que ficar sem a conexão de rede é problema para você..."

"Pode *apostar* que seria."

"...então enquanto estamos falando disso, vou dar o número do meu telefone celular. Se precisar, você pode ligar direto para mim."

"Isso seria ótimo."

"O número é 555-867-5309."

"555-867-5309. Entendi, obrigado. Qual é mesmo o seu nome?"

"É Eddie. Mais uma coisa, preciso verificar o número de porta ao qual o seu computador está conectado. Dê uma olhada no seu computador e veja se há uma etiqueta em algum lugar dizendo algo como 'Número de porta'."

"Espere um pouco... Não. não vejo nada parecido."

"OK, então na parte de trás do computador você consegue reconhecer o cabo de rede?"

"Sim."

"Veja onde ele está ligado. Veja se há uma etiqueta no conector ao qual ele está ligado."

"Espere um pouco. Sim, espere aí, tenho de me ajoelhar para chegar mais perto e ler, Muito bem, é a porta 6 traço 47."

"Bom, é isso o que tínhamos, só queria ter certeza,"

A segunda ligação: o cara de TI

Dois dias depois, uma ligação foi recebida no Centro de Operações de Rede da mesma empresa.

"Olá, aqui é Bob. Trabalho na Contabilidade do escritório de Tom DeLay. Estamos tentando solucionar um problema de cabo. Preciso desativar a Porta 6-47."

O rapaz de TI disse que isso seria feito em alguns minutos e pediu que eles avisassem quando poderiam ativar novamente a porta.

A terceira ligação: conseguindo ajuda do inimigo

Cerca de uma hora mais tarde, o suposto Eddie Martin estava fazendo compras na Circuit City quando seu telefone celular tocou. Ele verificou o número que estava ligando, viu que a chamada tinha sido feita do estaleiro e correu para um lugar tranqüilo antes de atender.

"Serviço ao Cliente. Eddie."

"Olá, Eddie. Estou ouvindo um eco, onde você está?"

'Estou em um gabinete de cabos. Quem está falando?"

"Aqui é Tom DeLay. Rapaz, estou feliz em falar com você. Talvez se lembre de mim, você me ligou outro dia. A minha conexão de rede acabou de cair como você disse que aconteceria e estou meio em pânico aqui."

"É, temos um monte de gente assim agora. Até o final do dia tudo estará resolvido. Tudo bem?"

"NÃO! Droga, vou me atrasar muito se tiver de esperar tanto. Qual é o melhor prazo que você tem para mim?"

"Qual é a sua urgência?"

"Posso fazer outras coisas agora. Há alguma chance de você consertar isso em meia hora?"

"MEIA HORA! Você não está querendo muito? Bem, vejamos, vou parar o que estou fazendo e ver se consigo resolver isso para você."

"Olha, obrigado mesmo, Eddie."

A quarta ligação: você conseguiu!

Quarenta e cinco minutos depois...

Tom? Aqui é o Eddie. Tente se conectar na rede agora.". Após alguns momentos:

"Ah, que bom está funcionando. Isso é ótimo."

"Bom, estou feliz que consegui cuidai disso para você."

"Sim, muito obrigado."

"Ouça. se quiser ter certeza de que a sua conexão não vai cair novamente, você precisa executar alguns softwares. Isso só vai levar uns minutos."

"Mas agora não é uma hora boa."

"Entendo... Mas isso poderia evitar grandes dores de cabeça para nós dois da próxima vez que esse problema de rede acontecesse de novo."

"Bom... se são apenas alguns minutos."

"Faça o seguinte..."

Eddie instruiu Tom para fazer o download de um pequeno aplicativo de um site Web. Após o programa ser carregado. Eddie disse a Tom para clicar duas vezes nele. Ele tentou, mas disse:

"Não está funcionando. Não está acontecendo nada."

"Ah. que pena. Deve haver algo de errado com o programa. Vamos nos livrar dele. podemos tentar novamente outra hora." E instruiu Tom para excluir o programa de modo que ele não pudesse ser recuperado.

Tempo total decorrido: doze minutos.

A história do atacante

Bobby Wallace sempre achou que era uma piada quando ele pegava um bom trabalho como esse e seu cliente evitava responder a pergunta que ninguém fazia, mas que era óbvia: por que eles queriam as informações. Neste caso, ele só podia imaginar dois motivos. Talvez eles representassem alguma organização que estava interessada em comprar a empresa-alvo, a Starboard, e quisessem saber exatamente qual era a sua situação financeira — particularmente todas aquelas coisas que o alvo poderia querer esconder do comprador em potencial. Ou talvez eles representassem investidores que achavam que havia algo de estranho no modo como o dinheiro estava sendo tratado e queriam descobrir se algum executivo poderia ser pego com "a mão na botija".

E talvez o seu cliente também não quisesse lhe dizer o verdadeiro motivo, porque se Bobby soubesse como as informações eram valiosas, ele provavelmente iria querer mais dinheiro para fazer o trabalho.

Existem várias maneiras de invadir os arquivos mais secretos de uma empresa. Bobby passou alguns dias pensando nas opções e fazendo algumas verificações antes de resolver que plano iria usar. Ele optou por um que pedia uma abordagem de que gostava muito, na qual o alvo é definido para pedir ajuda ao atacante.

Para os iniciantes, Bobby escolheu um telefone celular pré-pago de US$ 39,95, em uma loja de conveniência. Ele fez uma ligação para o homem que havia sido escolhido como seu alvo, fingiu ser do help desk da empresa e organizou as coisas para que o homem ligasse para o telefone celular de Bobby a qualquer momento que houvesse um problema com a sua conexão de rede.

Ele deu uma pausa de dois dias para não parecer tão óbvio e, em seguida, ligou para o centro de operações de rede da empresa (NOC). Ele disse que estava solucionando um problema para Tom, o alvo, e pediu que a conexão de rede de Tom fosse desligada. Bobby sabia que essa era a parte mais complicada de todo o plano — em muitas empresas, o pessoal do help desk trabalha junto com o NOC; na verdade, ele sabia que o help desk geralmente faz parte da organização de TI. Mas o indiferente rapaz do NOC com quem ele falou tratou a ligação como rotina, não pediu o nome do funcionário que deveria estar trabalhando no problema de rede e concordou em desativar a porta de rede do alvo, Quando tudo estava pronto. Tom estaria totalmente isolado da intranet da empresa, incapaz de recuperar arquivos do servidor, de trocar arquivos com seus colegas, de fazer o download das suas mensagens de correio eletrônico ou mesmo de enviar uma página de dados para a impressora. No mundo de hoje, isso é como morar em uma caverna.

Como Bobby esperava, não demorou muito para o seu celular tocar E claro que ele deu a impressão de estar disposto a ajudar esse pobre "colega de trabalho" com problemas. Em seguida, ligou para o NOC e fez com que a conexão de rede do homem voltasse. Finalmente, ele ligou para o homem e manipulou a sua credulidade mais uma vez, desta vez fazendo-o sentir-se culpado por dizer não depois que Bobby lhe havia prestado um favor. Tom concordou com a solicitação de descarregar um software no seu computador.

Aquilo com o qual ele concordou não era o que parecia. O software que Tom descarregou como algo que evitaria que a sua conexão fosse desligada era. na verdade, um *Cavalo de Tróia,* um aplicativo de software que fez no computador de Tom aquilo que a fraude original havia feito para os troianos: ele trouxe o inimigo para dentro do campo de batalha. Tom relatou que nada havia acontecido quando clicou duas vezes no ícone do software; o fato era que, por projeto, ele não veria nada acontecendo, embora o pequeno aplicativo estivesse instalando um programa secreto que permitiria ao inimigo infiltrado ocultar o acesso ao computador de Tom.

Jargão

Cavalo de Tróia **Um programa que contém um código malicioso ou prejudicial, criado para gerenciar os arquivos do computador da vítima ou para obter informações do computador ou da rede da vítima. Alguns deles foram criados para ocultar-se dentro do sistema operacional do computador e espiar cada tecla digitada ou ação, ou para aceitar instruções por uma conexão de rede para executar alguma função, tudo isso sem que a vítima tenha consciência da sua presença.**

Com o software em execução, Bobby leve o controle completo do computador de Tom através de uma aplicação-cliente repleta de *shells de comandos remotos.* Quando Bobby acessava o computador de Tom, ele podia procurar os arquivos da contabilidade que lhe interessavam e podia copiá-los. Em seguida, quando quisesse, ele poderia examiná-los para obter as informações que dariam a seus clientes aquilo que eles estavam procurando.

E isso não era tudo. Ele poderia voltar a qualquer momento para pesquisar as mensagens de correio eletrônico e os memorandos particulares dos executivos da empresa, poderia executar uma pesquisa de texto com as palavras que revelariam partes interessantes da informação.

Naquela noite, depois de enganar o seu alvo para que ele instalasse um Cavalo de Tróia, Bobby jogou o telefone celular em uma lata de lixo. Obviamente, ele teve o cuidado de limpar primeiro a memória e tirar a bateria — a última coisa que ele queria era que alguém ligasse para o número do celular por engano e fizesse o telefone tocar!

Analisando a trapaça

O atacante cria uma teia para convencer o alvo de que ele tem um problema que na verdade não existe --- ou, como neste caso, de um problema que ainda não aconteceu, mas que o atacante sabe que *acontecerá* porque ele vai causá-lo. Em seguida, ele se apresenta como a pessoa que pode fornecer a solução.

O cenário desse tipo de ataque é particularmente suculento para o atacante. Devido à semente plantada com antecedência, quando o alvo descobre que tem um problema, ele mesmo faz a ligação telefônica para implorar ajuda. O atacante só tem de se sentar e esperar que o telefone toque, uma tática conhecida na área como *engenharia social inversa.* Um atacante que consegue fazer o alvo ligar para *ele* ganha credibilidade constante. Se eu fizer uma ligação para alguém que acho que trabalha no help desk, não vou começar a pedir que ele prove a sua identidade. É nesse ponto que o atacante sabe que conseguiu.

Recado do Mitnick

Se um estranho lhe fizer um favor e depois pedir outro em troca, não faça nada sem antes pensar cuidadosamente naquilo que ele está pedindo.

Jargão

Shell de comandos remoto Uma interface não-gráfica que aceita comandos baseados em texto para executar determinadas funções ou executar programas. Um atacante que explora as vulnerabilidades técnicas ou que pode instalar um programa Cavalo de Tróia no computador da vítima pode obter o acesso remoto a um shell de comandos.

Engenharia social inversa Um ataque de engenharia social no qual o atacante cria uma situação na qual a vítima tem um problema e entra em contato com ele para obter ajuda. Outra forma de engenharia social inversa é aquela que se volta contra o atacante. O alvo reconhece o ataque e usa princípios psicológicos de influência para tirar o máximo possível de informações do atacante para que a empresa possa preservar os ativos visados.

Em um golpe como esse, o engenheiro social tenta escolher um alvo que tenha conhecimentos limitados de computadores. Quanto mais ele souber, maiores as chances de ele suspeitar ou descobrir que está sendo manipulado. Aquele que às vezes chamo de funcionário com um desafio de computador, que tem menos conhecimento da tecnologia e dos procedimentos, tem mais chances de colaborar. Ele tem mais chances de cair em uma armadilha do tipo "Basta fazer o download de um programa pequeno" porque não tem a menor idéia do dano em potencial que um programa de computador pode causar Alem disso, há uma chance bem menor de que ele entenda o valor das informações que estão na rede de computadores que ele está colocando em risco.

UMA AJUDAZINHA PARA O NOVO COLEGA

Os empregados novos são o alvo preferido dos atacantes. Eles ainda não conhecem muitas pessoas, não conhecem os procedimentos ou o que podem ou não fazer na empresa, E para causar uma boa impressão, eles estão ansiosos para mostrar como são prestativos e como podem ser rápidos.

A prestativa Andrea

"Recursos Humanos, Andrea Calhoun."

"Andrea, oi, aqui é Alex da Segurança Corporativa."

"Sim?"

"Como vai?"

"Tudo bem. Em que posso ajudá-lo?"

"Ouça, estamos desenvolvendo um seminário sobre segurança para os empregados novos e precisamos de algumas pessoas para fazer uma experiência. Preciso do nome e do número de telefone de todos os novos contratados do mês passado. Você pode me ajudar?"

"So terei essa lista esta tarde. Tudo bem? Qual é o seu ramal?"

"Claro, tudo bem, o ramal é 52... ah, mas vou estar em reunião na maior parte do dia. Ligo para você quando voltar ao escritório, talvez após as quatro."

Quando Alex ligou, lá pelas 16h30, Andrea já tinha a lista pronta e leu os nomes e os ramais,

Um recado para Rosemary

Rosemary Morgan estava encantada com o seu novo emprego. Ela nunca havia trabalhado antes em uma revista e estava achando as pessoas mais amigas do que havia imaginado, uma surpresa por causa da pressão interminável sofrida pela maioria da equipe sobre o prazo para entregar a edição do mês. A ligação que ela recebeu uma manhã de terça-feira reconfirmou essa impressão de amizade.

"É Rosemary Morgan?"

"Sim."

"Olá, Rosemary, Aqui é Bill Jorday do grupo de Segurança da Informação."

"Sim?"

"Alguém do nosso departamento já falou com você sobre as melhores práticas de segurança?"

"Acho que não."

"Bem, vejamos. Para os iniciantes, não permitimos que ninguém instale um software trazido de fora da empresa. Isso porque não queremos nenhum problema com software sem licença de uso. E também para evitar quaisquer problemas com software que tenha um worm ou um vírus."

Tudo bem."

"Você está a par das nossas políticas sobre correio eletrônico?"

"Não."

"Qual é o seu endereço de correio eletrônico atual?"

"Rosemary@ttrzine.net."

"O seu nome de usuário é Rosemary?"

"Não. É R-sublinhado-Morgan."

"Certo. Queremos que todos os nossos novos empregados saibam que pode ser perigoso abrir anexos de correio eletrônico que você não está esperando. Muitos dos vírus são enviados e chegam em mensagens de correio eletrônico que parecem vir de pessoas que você conhece. Assim sendo, se receber uma mensagem de correio eletrônico com um anexo que não está esperando, você deve sempre verificar se a pessoa relacionada na caixa de destinatário realmente enviou a mensagem. Você entendeu?"

"Sim, já ouvi falar disso."

"Bom. E a nossa política diz que você tem de mudar de senha a cada 90 dias. Qual foi a última vez que você mudou a sua senha?"

"Estou aqui há apenas três semanas; ainda estou usando a primeira senha que criei."

"Muito bem. Você pode aguardar o restante dos 90 dias. Mas precisamos ter certeza de que as pessoas estão usando senhas que não sejam muito fáceis de adivinhar. Você está usando uma senha formada por letras e números?"

"Não."

Temos de corrigir isso. Que senha você está usando agora?"

"O nome da minha filha: Annette."

"Essa não é mesmo uma senha segura. Você nunca deve escolher uma senha que se baseia em informações da família. Bem. vejamos... você poderia fazer o mesmo que eu. Você pode usar o que está usando agora como a primeira parte da senha, mas sempre que mudar você inclui um número para o mês atual."

"Então, se eu fizesse isso agora em março, eu usaria três ou zero três?"

"isso depende de você. Aquilo com o qual você se sentir mais à vontade."

"Acho que Annette-três."

"Bom. Você quer que eu diga como você faz para alterar a senha?"

"Não, eu sei como fazer isso."

"Bom. E mais uma coisa sobre a qual precisamos conversar. Você tem software antivírus no seu computador e é importante mantê-lo atualizado. Você nunca deve desativar a atualização automática, mesmo que o seu computador fique mais lento de vez em quando. Tudo bem?"

"É claro."

"Muito bom. E você tem o nosso número de telefone. Se tiver algum problema com o computador, é só nos ligar."

Ela não tinha o número. Ele deu-lhe o número, ela tomou nota e voltou a trabalhar novamente, feliz com o modo como se sentia bem cuidada.

Analisando a trapaça

Esta história reforça um tema básico que você encontrará aqui: a maioria das informações comuns que um engenheiro social quer de um empregado, independente do seu objetivo final, são as credenciais de autenticação do alvo. Com um nome de conta e uma senha em mãos de um único empregado na área certa da empresa, o atacante tem o que ele precisa para entrar e localizar as informações que está procurando. Ter essas informações é como encontrar as chaves do reino; com elas em mãos é possível mover-se livremente pelo espaço corporativo e encontrar o tesouro que se busca.

Recado do Mitnick

Antes que os empregados novos tenham acesso a qualquer sistema de computador da empresa, eles devem ser treinados para seguir as boas práticas de segurança, particularmente as políticas sobre nunca divulgar suas senhas.

NÃO TAO SEGURO QUANTO VOCÊ ACHA

"A empresa que não se esforça para proteger suas informações confidenciais é simplesmente negligente." Muitas pessoas concordam com essa declaração. E o mundo seria um lugar melhor se a vida não fosse tão óbvia e tão simples. A verdade é que mesmo essas empresas que se esforçam para proteger as informações confidenciais podem estar correndo um sério risco.

Esta é uma história que ilustra o modo como as empresas se enganam a cada dia, pensando que suas práticas de segurança criadas por profissionais experientes e competentes não podem ser burladas.

A história de Steve Cramer

Não era um grande gramado, não um daqueles gramados caros e bem plantados. Ele não despertava inveja. E certamente não era bastante grande para dar-lhe uma desculpa para comprar um cortador de grama elétrico, o que era bom, porque ele não teria usado uma de qualquer maneira. Steve gostava de cortar a grama com o cortador manual porque era mais longo e a tarefa era uma desculpa conveniente para concentrar-se em seus próprios pensamentos em vez de ouvir Anna contando as histórias das pessoas do banco onde ela trabalhava ou explicando as tarefas que ele teria de realizar. Ele odiava aquelas listas do que fazer que haviam se tomado parte integrante dos seus finais de semana. Ele lembrou-se daquele Pete de 12 anos que era esperto demais e conseguiu fazer parte da equipe de natação. Agora ele tinha de estar trabalhando ou em uma reunião todos os sábados para se livrar das tarefas do sábado.

Algumas pessoas poderiam achar que o trabalho de Steve, que criava novos dispositivos para a GeminiMed Medicai Products, era aborrecedor; mas ele sabia que estava salvando vidas. Steve imaginava a si mesmo como pertencente a uma linha criativa de trabalho. Artistas, compositores, engenheiros — no seu ponto de vista, todos eles enfrentavam o mesmo tipo de desafio que ele: eles

criavam algo que ninguém havia feito antes. E o seu mais recente e curioso tipo de *heart stent** seria a realização que lhe daria mais orgulho de todas.

Era quase 11 h30 da manhã naquele sábado, e Steve estava aborrecido porque já linha quase terminado de cortar a grama e ainda não havia feito nenhum progresso real para descobrir como reduzir os requisitos de energia do *heart stent,* a última barreira que restava. Um problema perfeito para ser resolvido enquanto se corta a grama, mas nenhuma solução havia surgido.

Anna apareceu na porta, com o cabelo coberto com o lenço xadrez de cowboy que ela usava para tirar o pó da casa. "Telefone", ela gritou para ele. "É alguém do trabalho."

"Quem?", perguntou Steve.

"Ralph alguma coisa, acho."

Ralph? Steve não conseguia se lembrar de alguém da GeminiMed chamado Ralph que poderia estar ligando em um final de semana. Mas Anna provavelmente havia entendido o nome errado.

"Steve, aqui é Ramon Perez, do Suporte Técnico". Ramon — como será que Anna conseguiu entender um nome tão diferente como Ralph, Steve se perguntava.

"Esta é apenas uma ligação de cortesia", Ramon dizia. "Três dos servidores estão paralisados, achamos que pode ser um vírus e temos de limpar as unidades de disco c restaurar do backup. Os seus arquivos estarão prontos na quarta ou quinta-feira com sorte."

"Isso não é possível", disse Steve com firmeza, tentando não se deixar tomar pela frustração. Como essas pessoas podiam ser tão estúpidas? Elas realmente achavam que ele poderia ficar sem acessar seus arquivos durante todo o final de semana e na maior parte da próxima semana? "De maneira nenhuma. Vou me sentar no meu terminal aqui em casa daqui a duas horas e preciso acessar meus arquivos. Isso está claro?"

"Sim. bem, todos para quem liguei até agora querem ser os primeiros da lista. Desisti do meu final de semana para vir trabalhar nisso e não é engraçado ter todo mundo com quem falo brigando comigo."

"Estou com um prazo curto, a empresa conta com isso; tenho de fazer o trabalho nesta tarde. Que parte disso você não entendeu?"

"Ainda tenho de ligar para muita gente antes de começar", retrucou Ramon. "E se eu dissesse que você terá os seus arquivos na terça?"

"Não na terça, não na segunda, hoje. AGORA!", disse Steve, tentando descobrir para quem ele ligaria se não conseguisse fazer esse cabeça dura entender.

"OK, OK", repetiu Ramon, e Steve o ouviu dar um suspiro de aborrecimento. "Vou ver o que posso fazer para que você não pare. Você usa o servidor RM22. certo?"

"O RM22 e o GM16. Os dois."

"Certo. OK, posso pular algumas etapas e economizar algum tempo — vou precisar do seu nome de usuário e senha."

Uh oh. Steve pensou. *O que está acontecendo? Por que ele precisa da minha senha? Por que o TI entre todas as pessoas pediria a senha?*

"Qual é o seu sobrenome e quem é o seu supervisor?"

* Heart Stent: projeto que une a informática e a medicina para desenvolver técnicas que estudam detalhes do coração e seu funcionamento, utilizando o que existe de mais modemo em tecnologia. (N.R.T.)

"Ramon Perez. Veja, quando você foi contratado, havia um formulário a preencher para obter uma conta de usuário e você tinha de colocar uma senha. Eu poderia procurar e mostrar que o temos no arquivo aqui. Tudo bem?"

Steve pensou alguns instantes e concordou. Ele desligou com impaciência cada vez maior, enquanto Ramon foi procurar os documentos em um arquivo. Finalmente ele voltou ao telefone, Steve podia ouvi-lo procurando na pilha de papéis.

"Ah, aqui está", disse finalmente Ramon. "Você colocou a senha 'Janice'."

Janice, Steve pensou. Esse era o nome da mãe e ele o havia usado algumas vezes como senha. Ele podia muito bem ter colocado essa senha ao preencher a documentação de contratação.

"Sim, está certo", ele reconheceu.

"OK, estamos perdendo tempo. Você sabe que não estou mentindo, quer que eu use o atalho e devolva seus arquivos rapidamente. Você vai me ajudar?"

"O meu ID é s, d, sublinhado, cramer — c-r-a-m-e-r. A senha é 'pelicano'."

"Vou começar imediatamente", afirmou Ramon, finalmente parecendo prestativo. "Só preciso de algumas horas."

Steve terminou o gramado, almoçou e quando voltou ao computador descobriu que, sem dúvida, seus arquivos haviam sido restaurados. Ele ficou feliz consigo mesmo por ter lidado com tanta energia com aquele funcionário pouco gentil do TI e esperava que Anna tivesse ouvido como ele foi positivo. Seria bom que Ramon ou o seu chefe recebessem uma advertência, mas ele sabia que isso era uma daquelas coisas com as quais ele nunca ia querer se envolver.

A história de Craig Cogburne

Craig Cogburne era vendedor de uma empresa de alta tecnologia e era um bom vendedor. Depois de um certo tempo ele começou a perceber que tinha habilidade para fazer a leitura de um cliente, entender quais eram os pontos de resistência da pessoa e reconhecer alguns pontos fracos ou vulnerabilidades que facilitavam o fechamento da venda. Ele começou a pensar em outras maneiras de usar esse talento, e o caminho o levou a um campo muito mais lucrativo: a espionagem corporativa.

Esse era um cargo quente. Não parecia que seria preciso muito tempo e esforço para pagar uma viagem para o Havaí. Ou talvez para o Taiti.

O rapaz que me contratou não me contou quem era o cliente, é claro, mas parecia ser alguma empresa que queria acabar com a concorrência em um salto único, rápido e fácil. Tudo que eu precisava fazer era obter os projetos e especificações de produto de um dispositivo novo chamado heart stent, independente do que fosse. A empresa chamava-se GeminiMed. Eu nunca ouvira falar dela, mas ela era uma das empresas da Fortune 500, com escritórios em meia dúzia de lugares — o que tomava o trabalho mais fácil do que em uma empresa na qual há boas chances de a pessoa com quem você está falando conhecer o funcionário que você diz ser e saber que você não *é* ele. Isso, como dizem os pilotos sobre uma colisão em pleno ar, pode arruinar todo o seu dia.

O meu cliente enviou-me um fax, uma parte de uma revista médica que dizia que a GeminiMed estava trabalhando em um heart stent com um novo desenho radical, o qual seria chamado de STH-100. Para ajudar, algum repórter já havia feito grande parte do trabalho para mim. Tinha uma coisa que eu precisava ter antes mesmo de começar: o nome do novo produto.

Primeiro problema: obter os nomes das pessoas da empresa que trabalhavam no STH-100 ou que precisariam ver os projetos. Assim sendo, liguei para a telefonista e disse: "Prometi para um funcionário do seu grupo de engenharia que eu entraria em contato com ele e não me lembro do seu sobrenome, mas o primeiro nome começava com S". Ela respondeu: "Temos Scott Archer e Sam Davidson." Fiz uma longa pausa. "Qual deles trabalha no grupo do STH-100?" Ela não sabia, e escolhi Scott Archer aleatoriamente. Ela fez a ligação.

Quando ele atendeu, comecei: "Olá, meu nome é Mike. da sala de correspondência. Tenho uma encomenda FedEx aqui para a equipe de projeto do Heart Stent STH-100. Você tem alguma idéia para quem mando?" Ele me deu o nome do líder do projeto, Jerry Mendel. Ele ate procurou o número do telefone na lista para mim,

Liguei. Mendel não estava lã, mas a mensagem na sua secretária eletrônica dizia que ele estava de férias até o dia 13, o que significava que ele tinha ainda mais uma semana para esquiar ou o que fosse, e todos que precisassem de alguma coisa nesse meio tempo deveriam ligar para Michelle no ramal 9137. Esse pessoal é muito prestativo, muito prestativo, sem dúvida.

Desliguei e liguei para Michelle: "Aqui *e* Bill Thomas, Jerry me disse para eu ligar quando tivesse as especificações para que a sua equipe examinasse. Você está trabalhando no *heart stent,* certo?" Ela disse onde eles estavam.

Agora estávamos chegando a parte mais interessante do golpe, Se ela começasse a suspeitar, eu estava pronto para jogar uma carta sobre como eu estava tentando fazer um favor que Jerry havia me pedido. Indaguei: "Em qual sistema você está?"

"Sistema?"

"Quais servidores de computador o seu grupo usa?"

"Ah, sim", ela disse, "o RM22. E algumas pessoas do grupo usam também o GM16".

Bom. Precisava disso e essa era uma informação que eu podia ter sem que ela suspeitasse de alguma coisa. Para que ela me desse a próxima informação falei o mais informalmente que pude. "Jerry disse que você me daria uma lista de endereços de correio eletrônico das pessoas da equipe de desenvolvimento." E prendi a respiração.

"Certo. A lista de distribuição é muito longa para eu ler, posso enviá-la por correio eletrônico para você?"

Opa! Qualquer endereço de correio eletrônico que não terminasse com GeminiMed.com seria uma imensa bandeira vermelha. "Você pode me enviar por fax?", perguntei.

Ela não viu nenhum problema nisso.

"O nosso aparelho de fax está com problemas. Vou lhe dar o número de outro. Já ligo de volta". afirmei e desliguei.

Você deve achar que tinha um problema complicado aqui, mas esse é apenas outro truque de rotina dos negócios. Esperei um pouco para que a minha voz não fosse reconhecida pela recepcionista e, em seguida, liguei: "Oi, meu nome é Bill Thomas, o nosso aparelho de fax não está funcionando, posso pedir para enviarem um fax para a sua máquina?" Ela disse que sim e me deu o número.

Eu poderia ir lá e pegar o fax, certo? E claro que não. Primeira regra: nunca visite as instalações, a menos que isso seja absolutamente necessário. Eles têm muita dificuldade em identificá-lo se for apenas uma voz ao telefone. E se não puderem identificá-lo, eles não podem prendê-lo. E difícil algemar uma voz. Assim sendo, liguei para ela depois de algum tempo e perguntei se o meu fax havia chegado, "Sim", respondeu.

"Olhe", salientei, "tenho de enviar isso para um consultor que estamos usando, Você poderia enviar o fax para mim?" Ela concordou. E por que não — como uma recepcionista poderia reconhecer informações confidenciais? Enquanto ela enviava o fax para o "consultor", fiz a minha caminhada diária ate uma loja de serviços de escritório próxima da minha casa, aquela que tem uma placa dizendo "Enviamos e recebemos faxes". O meu fax deveria chegar antes de mim e, como esperava, ele estava lá me aguardando quando cheguei. Seis páginas por US$ 1,75. Por uma nota de US$ 10 mais o troco tinha toda a lista de nomes e endereços de correio eletrônico do grupo.

Entrando

Muito bem, já havia falado com três ou quatro pessoas diferentes em apenas algumas horas e já estava um passo de gigante mais próximo de entrar nos computadores da empresa, Mas precisava de mais algumas informações antes de estar em casa.

A informação número um era o número de discagem externa do servidor da Engenharia. Liguei novamente para a GeminiMed e pedi a telefonista para falar com o Departamento de TI. Para o funcionário que atendeu, pedi para falar com alguém que pudesse me dar ajuda com computadores. Ele me transferiu e fingi me confundir e ser meio estúpido com qualquer coisa técnica. "Estou em casa, acabei de comprar um laptop novo e preciso configurá-lo para poder discar de fora."

O procedimento era óbvio, mas deixei pacientemente que ele me instruísse até que eu conseguisse o número de discagem. Ele me deu o número como mais uma informação de rotina. Em seguida, pedi para ele esperar e experimentei. Perfeito!

Agora eu já havia superado o problema de me conectar à rede. Disquei e descobri que eles estavam configurados com um servidor de terminal que permitia me conectar a qualquer computador da sua rede interna. Após muitas tentativas, encontrei o computador de alguém que tinha uma conta de convidado que não exigia senha. Alguns sistemas operacionais quando são instalados pela primeira vez orientam o usuário para configurar um ID e uma senha, mas também fornecem uma conta de convidado. O usuário deve definir sua própria senha para a conta de convidado ou desativá-la, mas a maioria das pessoas não sabe disso ou não quer saber. Esse sistema provavelmente acabara de ser configurado e o proprietário não tinha se dado ao trabalho de desativar a conta de convidado.

Graças à conta de convidado, agora eu tinha acesso a um computador, o qual por acaso executava uma versão mais antiga do sistema operacional UNIX. No UNIX, o sistema operacional mantém um arquivo de senha que contem as senhas criptografadas de todos que estão autorizados a acessar aquele computador O arquivo de senhas contém o *hash* de uma via (ou seja, uma forma de criptografia que é irreversível) da senha de cada usuário. Com um hash de uma via, uma senha real "justdoit", por exemplo, seria representada como um hash na forma criptografada; neste caso, o hash seria convertido pelo UNIX em treze caracteres alfanuméricos,

Quando Billy Bob quer transferir alguns arquivos para um computador, ele deve identificar a si mesmo fornecendo um nome de usuário e uma senha. O programa do sistema que verifica essa

Jargão

Senha hash **Uma string de coisas ininteligíveis que resulta do processamento de uma senha por meio de um processo de criptografia de uma via. O processo deve ser irreversível; ou seja, acredita-se que não é possível reconstruir a senha a partir do hash.**

autorização criptografa a senha que ele insere e, em seguida, compara o resultado com a senha criptografada (o hash) contida no arquivo de senhas. Se as duas coincidirem, o acesso é concedido.

Como as senhas do arquivo estavam criptografadas, o arquivo em si foi disponibilizado para todo usuário com base na teoria de que não há um modo conhecido de decriptografar as senhas. Isso é uma piada — eu fiz o download do arquivo, executei um ataque de senhas automatizadas *(brute force attacks)* nele (consulte o Capítulo 12 para obter mais informações sobre esse método) e descobri que um dos engenheiros da equipe de desenvolvimento, um funcionário chamado Steven Cramer, no momento tinha uma conta no computador com a senha "Janice". Só por acaso, tentei entrar na sua conta com aquela senha em um dos servidores de desenvolvimento. Se isso funcionasse, teria economizado algum tempo e um pouco de risco. Mas isso não funcionou.

Isso significava que eu tinha de fazer o rapaz me dizer o seu nome de usuário e senha. Para tanto, teria de esperar até o final de semana.

Você já sabe o resto. No sábado, liguei para Cramer e contei a história sobre um vírus e os servidores que tinham de ser restaurados do backup para superar a sua suspeita.

E sobre a tal história que contei para ele, aquela sobre a senha que ele deu quando preencheu a sua documentação de funcionário? Estava contando com o fato de que ele não se lembraria que isso nunca aconteceu. Um empregado novo preenche tantos formulários que, anos mais tarde, quem iria se lembrar? E de qualquer forma, se tivesse de desistir dele, ainda teria aquela longa lista com outros nomes.

Com o seu nome de usuário e senha, entrei no servidor, pesquei um pouco e. em seguida, localizei os arquivos de projeto do STH-100. Não tinha muita certeza sobre quem eram as pessoas mais importantes e, assim, transferi todos os arquivos para um *dead drop,* um site FTP grátis na China, no qual eles podiam ser armazenados sem levantar suspeitas de ninguém. Deixe que o cliente procure em tudo e encontre o que ele quer.

Analisando a trapaça

Para o homem que estamos chamando de Craig Cogbure ou para qualquer pessoa como ele, com habilidades semelhantes nas artes do roubo que nem sempre são ilegais da engenharia social, o desafio apresentado aqui era quase que rotineiro. Seu objetivo era localizar e fazer o download dos arquivos armazenados em um computador corporativo seguro, protegido por um firewall e por toda a tecnologia normal de segurança.

A maioria do seu trabalho era tão fácil quanto recolher água da chuva em um barril. Ele começou fazendo-se passar por alguém da sala de correspondência e impôs uma sensação extra de urgência dizendo que havia um pacote do FedEx aguardando para ser entregue. Essa fraude forneceu o nome do chefe da equipe do grupo de engenharia do *heart stent,* o qual estava em férias, mas — como era

Jargão

Dead drop **Um lugar para deixar as informações, no qual é pouco provável que sejam encontradas por outras pessoas. No mundo dos espiões tradicionais, isso poderia estar atrás de um tijolo falso na parede; no mundo dos hackers de computadores, é comum haver um site da Internet em um país remoto.**

conveniente para qualquer engenheiro social que estava tentando roubar informações — ele havia deixado o nome e número de telefone da sua assistente. Ao ligar para ela, Craig eliminou todas as suspeitas dizendo que estava atendendo a uma solicitação do chefe da equipe. Com o chefe da equipe fora da cidade, Michelle não tinha como verificar essa solicitação. Ela aceitou-a como verdadeira e não teve problemas para fornecer uma lista das pessoas do grupo — para Craig, esse era um conjunto de informações necessário e muito valioso.

Ela nem suspeitou quando Craig quis que a lista fosse enviada por fax e não por correio eletrônico, o qual seria mais conveniente para ambos os lados. Por que ela foi tão crédula? Assim como muitos outros empregados, ela não queria que o seu chefe voltasse e descobrisse que ela havia impedido uma pessoa que estava apenas tentando fazer algo que o chefe havia pedido para ele fazer. Além disso, o interlocutor disse que o chefe não apenas autorizou a solicitação, como também pediu o seu auxílio. Novamente, este é um exemplo de alguém que tem um forte desejo de fazer parte de uma equipe, o que torna as pessoas mais sujeitas à fraude.

Craig evitou o risco de entrar fisicamente no prédio fazendo com que o fax fosse enviado para a recepcionista e sabendo que talvez ela ajudaria. Afinal, as recepcionistas são selecionadas por suas personalidades charmosas e por sua capacidade de causar uma boa impressão. Fazer pequenos favores como receber um fax e enviá-lo é algo que se espera da recepcionista. Craig aproveitou-se desse fato. Aquilo que ela estava enviando seriam informações que poderiam ter tocado o alarme para qualquer pessoa que conhecesse o valor das informações — mas como uma recepcionista poderia saber quais informações são inofensivas e quais são confidenciais?

Usando um estilo diferente de manipulação, Craig agiu como alguém confuso e ingênuo para convencer o funcionário das operações de computadores a fornecer o número de acesso por discagem para o servidor de terminal da empresa, o hardware usado como um ponto de conexão com os outros sistemas de computadores dentro da rede interna.

Recado do Mitnick

A prioridade de todos que trabalham é fazer o trabalho. Sob essa pressão, as práticas de segurança em geral ficam em segundo plano e são desprezadas ou ignoradas. Os engenheiros sociais usam isso ao praticarem sua arte.

Craig pode se conectar facilmente tentando uma senha-padrão que nunca havia sido alterada, uma das enormes lacunas que existem em muitas redes internas que usam a segurança de firewall. Na verdade, as senhas-padrão de muitos sistemas operacionais, roteadores e outros tipos de produtos, entre eles os PBXs, estão disponíveis on-line. Todo engenheiro social, hacker ou espião industrial. bem como os simples curiosos, pode encontrar a lista em http://www.phenoelit.de/dpl/dpl.html. (É absolutamente inacreditável como a Internet facilita a vida daqueles que sabem onde procurar. E *você* também sabe!)

Em seguida, Cogburne conseguiu convencer um homem cauteloso e desconfiado ("Como é o seu sobrenome? Quem é o seu supervisor?") a divulgar o seu nome de usuário e a sua senha para que ele pudesse acessar os servidores usados pela equipe de desenvolvimento do heart stent. Isso foi como deixar Craig com uma porta aberta para pesquisar nos segredos mais bem guardados da empresa e fazer o download dos planos do novo produto.

E se Steve Cramer continuasse suspeitando da ligação de Craig? É pouco provável que ele pudesse fazer alguma coisa quanto a relatar as suas suspeitas até aparecer no trabalho na segunda-feira e, então, já seria tarde demais para evitar o ataque.

Um segredo da última parte do plano: Craig a princípio se fez passar por indiferente e desinteressado nas preocupações de Steve e, em seguida, mudou o tom e pareceu estar ajudando Steve a fazer o seu trabalho. Na maior parte do tempo, se a vítima acredita que você está tentando ajudá-lo ou prestar-lhe algum tipo de favor, ela compartilhará das informações confidenciais que, de outra forma, teriam sido protegidas.

EVITANDO A TRAPAÇA

Um dos truques mais poderosos do engenheiro social envolve a virada da mesa. Foi isso que você viu neste capitulo. O engenheiro social cria o problema e, em seguida, o resolve num passe de mágica, enganando a vítima para que ela forneça o acesso aos segredos mais bem guardados da empresa. Os seus empregados seriam pegos nesse tipo de golpe? Você já teve o trabalho de escrever e distribuir regras específicas de segurança para ajudar a evitar isso?

Educar, educar e educar...

Existe uma velha história sobre um visitante de Nova York que pára um homem na rua e pergunta: "Como vou ao Carnegie Hall?" O homem responde: "Prática, prática, prática." Todos são tão vulneráveis aos ataques da engenharia social que a única defesa efetiva de uma empresa é educar e treinar o seu pessoal, dando-lhes a prática de que precisam para identificar um engenheiro social. E, em seguida, ela deve continuar lembrando sempre o pessoal daquilo que eles aprenderam no treinamento. mas que podem esquecer facilmente.

Todos da organização devem ser treinados para ter um grau apropriado de suspeita e cuidado ao serem contactados por alguém que não conhecem pessoalmente, sobretudo quando alguém pede algum tipo de acesso a um computador ou rede. É da natureza humana querer confiar nos outros, mas com dizem os japoneses, os negócios são uma guerra. Os seus negócios não podem permitir que você baixe a guarda. A política de segurança corporativa deve definir claramente o comportamento apropriado e inapropriado.

A segurança não tem tamanho único. O pessoal dos negócios tem regras e responsabilidades diferentes e cada posição tem vulnerabilidades próprias. Deve haver um nível básico de treinamento que todos da empresa devem ter e, depois, as pessoas também devem ser treinadas de acordo com o perfil do seu cargo para seguir determinados procedimentos que reduzem as chances de elas se tornarem parte do problema. As pessoas que trabalham com informações confidenciais ou que são colocadas em posições de confiança devem ter treinamento especializado adicional.

Mantendo seguras as informações confidenciais

Quando as pessoas são abordadas por um estranho que oferece ajuda, como vimos neste capítulo, elas têm de recorrer à política de segurança corporativa feita de acordo com as necessidades dos negócios, o tamanho e a cultura da sua empresa.

Nunca coopere com um estranho que pede para você procurar informações, digitar comandos desconhecidos em um computador, fazer alterações nas configurações do software ou — o mais

desastroso de tudo — abrir um anexo de correio eletrônico ou fazer o download de um software sem verificação. Todo programa de software — mesmo aquele que parece não fazer nada — pode não ser tão inocente quanto parece ser.

Observação

Não acredito que nenhuma empresa deva permitir qualquer troca de senhas. É muito mais fácil estabelecer uma regra que proíbe o pessoal de compartilhar ou trocar as senhas confidenciais. Isso também é mais seguro. Mas cada empresa tem de avaliar a sua própria cultura e as suas questões de segurança para fazer essa opção.

Existem determinados procedimentos que, independentemente de um bom treinamento, fazem com que fiquemos descuidados com o tempo. Nos esquecemos também daquele treinamento nos momentos de pressão, justamente quando precisamos dele. Você pensa que não dar o seu nome de conta e senha é uma regra que todo mundo sabe (ou deveria saber) e que nem é preciso dizer isso: é uma questão de bom senso. Mas, na verdade, cada empregado precisa ser freqüentemente lembrado de que o fornecimento de um nome de conta e uma senha do computador do escritório, do computador em casa ou mesmo da máquina de postagem na sala de correspondência *é* como dar o número do cartão eletrônico do banco.

Eventualmente — *muito* eventualmente — existe uma circunstância na qual é preciso, talvez até mesmo importante, dar a outra pessoa as informações confidenciais. Por esse motivo, não é apropriado criar uma regra absoluta sobre "nunca". Mesmo assim, as suas políticas e os seus procedimentos de segurança precisam ser muito específicos sobre as circunstâncias nas quais um empregado pode dar a sua senha e. o mais importante, sobre quem está autorizado a pedir essas informações.

Leve em conta a fonte

Na maioria das organizações, a regra deve ser de que todas as informações que possam causar danos à empresa ou a um colega de trabalho só possam ser dadas a alguém que se conhece pessoalmente ou cuja voz seja familiar e possa ser reconhecida sem dúvidas.

Nas situações de alta segurança, as únicas solicitações que devem ser concedidas são aquelas entregues pessoalmente ou com uma forma sólida de autenticação — por exemplo, dois itens separados, tais como um segredo compartilhado e um token baseado em tempo.

Os procedimentos de classificação de dados devem designar que *nenhuma* informação seja fornecida de uma parte da organização envolvida com trabalho confidencial para ninguém que não seja conhecido pessoalmente ou autenticado de alguma maneira.

Assim sendo, como você trata de uma solicitação aparentemente legítima de informações feita por outro empregado da empresa, tal como a lista de nomes e endereços de correio eletrônico das pessoas do seu grupo? Na verdade, como você aumenta a consciência para que um item como esse que é menos valioso do que, digamos, uma folha de especificações de um produto em desenvolvimento, seja reconhecido como algo que deve ser usado apenas internamente? Uma grande parte da solução é designar os empregados de cada departamento que tratarão de todas as solicitações de informações a serem enviadas para fora do grupo. Um programa avançado de treinamento em segurança deve ser fornecido para conscientizar esses empregados sobre os procedimentos especiais de verificação que devem ser seguidos.

Observação

Por incrível que pareça, mesmo procurando o nome e número de telefone do interlocutor no banco de dados de empregados da empresa e ligar para ele não é garantia absoluta — os engenheiros sociais conhecem maneiras de plantar nomes em um banco de dados corporativo ou de redirecionar as ligações telefônicas.

Não se esqueça de ninguém

Todos podem identificar as repartições dentro da sua empresa que precisam de um alto grau de proteção contra os ataques maliciosos. Mas, com freqüência, desprezamos os outros lugares que são menos óbvios, embora altamente vulneráveis. Em uma dessas histórias, a solicitação de que um fax fosse enviado para um número de telefone dentro da empresa parecia inocente e segura, embora o atacante tenha se aproveitado desse buraco na segurança. A lição é: todos, desde as secretárias e os assistentes administrativos até os executivos da empresa e os gerentes de primeiro escalão, precisam ter um treinamento especial em segurança, para que possam estar alertas para esses tipos de traques. E não se esqueça de fechar a poria da frente. Os recepcionistas também são alvos primários dos engenheiros sociais e também devem ter consciência das técnicas fraudulentas usadas por alguns visitantes e interlocutores.

A segurança corporativa deve estabelecer um único ponto de contato central para os empregados que acham que estão sendo alvo de um traque de um engenheiro social. Um único lugar para relatar incidentes de segurança fornece um sistema de avisos que deixará claro quando um ataque coordenado está em andamento, para que todo o dano possa ser imediatamente controlado.

Capítulo 6

Você Pode me Ajudar?"

Você viu como os engenheiros sociais enganam as pessoas oferecendo ajuda. Outra abordagem preferida é a virada da mesa: o engenheiro social age fingindo que precisa da ajuda da pessoa. Todos podemos simpatizar com as pessoas que estão precisando de ajuda, e a abordagem é sempre eficaz, permitindo que um engenheiro social atinja o seu objetivo.

O ESTRANHO NA CIDADE

Uma história do Capítulo 3 mostrou como um atacante pode convencer uma vítima a revelar o seu número de empregado. Esta usa uma abordagem diferente para conseguir o mesmo resultado e, em seguida, mostra como o atacante pode utilizar aquelas informações.

Continuando com os Jones

No Vale do Silício, existe uma determinada empresa global. Os escritórios de vendas espalhados e outras instalações de campo em todo o mundo estão conectados à sede daquela empresa por meio de uma WAN, uma rede de área remota. O intruso, um rapaz esperto chamado Brian Atterby, sabia que quase sempre era mais fácil invadir uma rede em um dos sites remotos no qual a segurança, quase com toda a certeza, é mais relaxada do que na sede.

O intruso ligou para o escritório de Chicago e pediu para falar com o Sr. Jones. A recepcionista perguntou se ele sabia qual era o primeiro nome do Sr. Jones e ele respondeu: "Tenho aqui, estou procurando. Quantos Jones você tem?" Ela afirmou: "Três. Em qual departamento ele trabalha?"

Ele continuou: "Se você me disser os nomes talvez eu o reconheça." E ela fez isso: "Barry, Joseph e Gordon."

"Joe. Tenho certeza de que era esse", salientou. "E ele trabalha em... qual departamento?"

"Desenvolvimento de Negócios."

"Muito bom. Você pode fazer a ligação, por favor?"

Ela completou a ligação. Quando o Jones atendeu, foi a vez do atacante: "Sr. Jones? Oi, aqui e Tony, da Folha de Pagamentos. Acabamos de concluir a sua solicitação para que o seu cheque de pagamento seja depositado diretamente na sua conta no Credit Union."

"O QUÊ???!!! Você deve estar brincando. Nunca fiz uma solicitação dessas. Nem tenho conta no Credit Union."

"Ah, droga. Já concluí a transação."

Jones ficou mais do que aborrecido com a idéia de que o seu pagamento poderia ir para a conta de outra pessoa, e estava começando a pensar que o rapaz do outro lado da linha devia ser meio lento. Antes mesmo de ele responder, o atacante continuou: "É melhor eu ver o que aconteceu. As alterações na folha de pagamento são inseridas pelo número de empregado. Qual é o seu número de empregado?"

Jones deu o número. O interlocutor disse: "Não, você está certo. A solicitação não veio de você. então." Jones pensou: "Eles estão ficando mais burros a cada ano."

"Olhe, vou cuidar disto. Vou fazer a correção agora mesmo. Não se preocupe, você receberá o seu próximo cheque de pagamento", disse o rapaz com segurança.

Uma viagem de negócios

Não muito depois disso, o administrador de sistemas da empresa no escritório de vendas em Austin, no Texas, recebeu uma ligação telefônica. "Aqui é Joseph Jones", anunciou o interlocutor. "Trabalho no departamento de Desenvolvimento de Negócios. Estarei na cidade por uma semana, no Driskill Hotel. Gostaria que você me configurasse uma conta temporária para eu acessar meu correio eletrônico sem precisar fazer uma ligação interurbana."

"Me dê novamente o seu nome e o seu número de empregado", pediu o administrador de sistemas. O falso Jones deu o número e continuou: "Você tem números de discagem rápida?"

"Espere um pouco. Tenho de verificar as informações no banco de dados." Depois de algum tempo ele disse: "OK, Joe. Diga-me qual é o número do seu prédio?" O atacante havia feito tudo direito e tinha a resposta na ponta da língua.

Recado do Mitnick

Não dependa das salvaguardas e firewalls de rede para proteger as suas informações. Olhe o seu ponto mais vulnerável. Geralmente você descobre que aquela vulnerabilidade está no seu pessoal.

"Muito bem", o administrador de sistemas afirmou, "você me convenceu".

Foi tudo muito simples. O administrador de sistemas havia verificado o nome de Joseph Jones, o departamento e o número de empregado e "Joe" havia dado a resposta certa para a pergunta de teste. "O seu nome de usuário será igual ao seu nome na corporação, jbjones", explicou o administrador de sistemas, "e eu vou lhe dar a senha inicial 'changeme'".

Analisando a trapaça

Com algumas ligações e gastando quinze minutos, o atacante havia ganhado acesso à rede de área remota da empresa. Essa era uma empresa que, como muitas outras, tinha aquilo que eu chamava de *segurança suave.* Essa descrição foi usada pela primeira vez por dois pesquisadores da Bell Labs, Steve Bellovin e Steven Cheswick. Eles descreveram essa segurança como "uma concha dura que se esmigalha com um núcleo macio como chiclete" — como um confeito. A concha externa, o firewall, argumentavam Bellovin e Cheswick. não representa proteção suficiente, porque após um invasor

Jargão

SEGURANÇA SUAVE (Candy Security) Um termo criado por Bellovin e Cheswick da Bell Labs para descrever um cenário de segurança no qual o perímetro externo (tal como um firewall) é forte, mas a infra-estrutura é fraca. O termo refere-se ao confeito, que tem uma casca externa dura e um centro mole.

conseguir contorná-la, os sistemas internos de computadores têm a segurança macia e mastigável. Na maior parte do tempo eles têm uma proteção inadequada.

Esta história coincide com a definição. Com um número de discagem e uma conta, o atacante nem precisava tentar passar pelo firewall da Internet e, depois que ele estava lá dentro, podia facilmente comprometer a maior parte dos sistemas da rede interna.

Segundo as minhas fontes, acho que um golpe semelhante foi dado em um dos maiores fabricantes de software para computadores do mundo. Você acharia que os administradores dessa empresa estariam treinados para detectar esse tipo de golpe? Mas de acordo com a minha experiência, ninguém está completamente seguro quando um engenheiro social é bastante inteligente e persuasivo.

SEGURANÇA SPEAKEASY

Nos velhos tempos do speakeasy — naqueles nightclubs da era da Lei Seca, onde acontecia o comércio ilegal de bebida alcoólica —, um provável cliente era admitido batendo à porta. Após alguns minutos, a porta se abria e um rosto forte e intimidador aparecia. Se o visitante era conhecido, ele podia falar o nome de algum patrono freqüentador do lugar ("Joe me mandou" era o suficiente) e o grandalhão lá dentro destrancava a porta e permitia a sua entrada.

O verdadeiro truque estava em saber a localização do speakeasy porque a porta não tinha placas, e os proprietários não penduravam sinais de néon para marcar a sua presença. Na maior parte dos casos, bastava aparecer no lugar certo para entrar. Infelizmente, o mesmo grau de salvaguarda e aplicado amplamente no mundo corporativo e fornece um nível de desproteção que eu chamo de *segurança speakeasy.*

Eu vi isso no cinema

Aqui está um exemplo de um filme meu preferido que muitas pessoas devem lembrar. No filme *Os Três Dias do Condor,* o personagem central, Turner (interpretado por Robert Redford), trabalha em uma pequena empresa de pesquisa contratada pela CIA. Um dia ele volta do almoço e descobre que todos os

Jargão

SEGURANÇA SPEAKEASY A segurança que depende do conhecimento do lugar onde estão as informações desejadas e do uso de uma palavra ou nome para acessar aquelas informações ou um sistema de computador,

seus colegas foram assassinados. Ele está sozinho para descobrir quem fez isso e por quê. Todo o tempo ele sabia que os assassinos, independentemente de quem eles fossem, estavam procurando por ele.

Mais tarde Turner consegue o número de telefone de um dos bandidos. Mas quem é essa pessoa. e como Turner pôde descobrir a sua localização? Ele tem sorte. O autor do roteiro, David Rayfiel, deu a Turner uma experiência que incluía o treinamento como técnico em telefonia no Exército, o que lhe dava o conhecimento das técnicas e práticas da empresa de telefonia. Com o número do telefone do assassino em mãos, Turner sabia exatamente o que fazer. No filme a cena é esta:

> TURNER DESLIGA E DISCA NOVAMENTE PARA OUTRO NÚMERO. TRIM! TRIM! Em seguida:
>
> **VOZ DE MULHER** *(FILTRO)*
>
> CNA. Sra. Coleman.
>
> **TURNER** *(no aparelho de leste)*
>
> Aqui é Harold Thomas, Sra. Coleman. Serviço ao Cliente. CNA de 202-555-7389, por favor.
>
> **VOZ DE MULHER** *(FILTRO)*
>
> Um momento, por favor.
>
> *(quase ao mesmo tempo)*
>
> Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland.

Ignorando o fato de que o roteirista usou por engano um código de área de Washington. D.C. para um endereço em Maryland, você já pode adivinhar o que aconteceu, não é?

Devido ao seu treinamento como técnico em telefonia, Turner sabia para qual número deveria discar para falar com um escritório da empresa chamado CNA, o escritório de Nome e Endereço de Clientes. O CNA foi montado para a conveniência dos instaladores e de outro pessoal autorizado pela empresa de telefonia. Um instalador pode ligar para o CNA e dar um número de telefone. O funcionário do CNA responde fornecendo o nome da pessoa à qual pertence o telefone daquele endereço.

Enganando a empresa de telefonia

No mundo real. o número de telefone do CNA é um segredo guardado a sete chaves. Embora as empresas de telefonia finalmente tenham aprendido e hoje em dia são menos generosas na divulgação fácil dessas informações, na época elas eram operadas com base em uma variação da segurança speakeasy, a qual é chamada pelos especialistas de segurança da informação de *segurança através da obscuridade.* Elas presumiam que os todos que ligassem para o CNA e conhecessem a linguagem

Jargão

A SEGURANÇA ATRAVÉS DA OBSCURIDADE Um método eficaz de segurança de computadores que mantém em segredo os detalhes de como funciona o sistema (protocolos, algoritmos e sistemas internos). A segurança através da obscuridade baseia-se na falsa suposição de que ninguém que esteja fora de um grupo de pessoas de confiança poderá enganar o sistema.

apropriada ("Serviço ao cliente. CNA de 555-1234, por favor", por exemplo) eram pessoas autorizadas a terem as informações.

Recado do Mitnick

A segurança através da obscuridade não tem *nenhum* efeito para bloquear os ataques da engenharia social. Todo sistema de computadores do mundo tem pelo menos um ser humano que o usa. Assim sendo, se o atacante puder manipular as pessoas que usam os sistemas, a obscuridade do sistema é irrelevante.

Não há necessidade de verificar ou identificar a si mesmo, nem dar um número de empregado, tampouco mudar uma senha diariamente. Se souber o número para o qual ligar e parecer autêntico, então terá direito às informações.

Essa não era uma suposição muito sólida por parte da empresa de telefonia. O seu único esforço de segurança era alterar o número do telefone periodicamente (pelo menos uma vez por ano). Mesmo assim, o número atual em determinado momento era amplamente conhecido entre os phreakers, os quais adoravam aproveitar essa conveniente fonte de informações e compartilhar os métodos de como fazer isso com seus colegas. O truque do CNA foi uma das primeiras coisas que aprendi quando fui apresentado ao hobby dos trotes de telefone ainda na adolescência.

Em todo o mundo dos negócios e no governo, a segurança speakeasy ainda prevalece. É provável que um invasor qualquer com algumas habilidades se faça passar por uma pessoa autorizada unindo informações suficientes sobre os departamentos, as pessoas e a linguagem da sua empresa. Às vezes menos do que isso é necessário: às vezes um número interno de telefone basta.

O GERENTE DE COMPUTADORES DESCUIDADO

Embora muitos empregados das organizações sejam negligentes, despreocupados ou não tenham conhecimento dos perigos para a segurança, você espera que alguém no cargo de gerente do centro de computadores de uma corporação da *Fortune 500* tenha conhecimento completo sobre as melhores práticas de segurança, certo?

Você não esperaria que um gerente do centro de computadores — alguém que faz parte do Departamento de Tecnologia da Informação da sua empresa — fosse vítima de um jogo de trapaça da engenharia social simplista e óbvio. *Particularmente* não se o engenheiro social é pouco mais do que uma criança, mal saindo da adolescência. Mas às vezes as suas expectativas podem estar erradas.

Sintonizando

Há anos um passatempo divertido para muitas pessoas era manter o rádio sintonizado na freqüência da polícia ou do corpo de bombeiros local para eventualmente ouvir as conversações sobre um roubo de banco em andamento, um prédio de escritórios em chamas ou uma caçada em alta velocidade à medida que o evento se desenrolava. As freqüências de rádio usadas pelos departamentos de policia e pelos bombeiros não estavam disponíveis em livros na livraria da esquina; hoje em dia eles são fornecidos em listagens da Web e em um livro que você compra na Radio Shack — as freqüências da polícia municipal, estadual e, em alguns casos, da federal.

Obviamente, não apenas os curiosos ouviam. Os ladrões que roubavam uma loja no meio da noite podiam sintonizar e ouvir se um carro de polícia estava sendo enviado para o local. Os traficantes de drogas podiam verificar as atividades dos agentes da Delegacia de Narcóticos local. Um incendiário podia aumentar o seu prazer doentio acendendo uma chama e ouvindo todo o tráfego pelo rádio enquanto os bombeiros lutavam para apagar o incêndio.

Nos últimos anos, o desenvolvimento da tecnologia dos computadores possibilitou a criptografia das mensagens por voz. A medida que os engenheiros encontravam maneiras de colocar cada vez mais poder de computação em um único microchip, eles começaram a criar pequenos rádios criptografados para os departamentos de polícia, os quais evitavam que os bandidos e os curiosos ouvissem.

Danny, o hacker benigno

Um hacker entusiasmado e habilidoso que chamaremos de Danny resolveu descobrir um modo de colocar as mãos em um software de criptografia supersecreto — o código-fonte — de um dos principais fabricantes de sistemas de rádio de segurança. Ele esperava que um estudo do código o ensinasse como enganar a polícia e talvez também pudesse usar a tecnologia para que até mesmo os departamentos do governo mais poderosos tivessem dificuldades em monitorar as suas conversas com seus amigos.

Os dannys do mundo sombrio dos hackers pertencem a uma categoria especial que se classifica em algum lugar entre os meramente curiosos, mas totalmente inofensivos, e os perigosos. Os dannys têm o conhecimento do especialista, combinado ao desejo maligno do hacker de invadir os sistemas e as redes pelo desafio intelectual e pelo prazer de descobrir como a tecnologia (funciona. Mas as suas acrobacias eletrônicas de invasão não passam disso — acrobacias. Esse pessoal, esses hackers benignos, entram ilegalmente nos sites simplesmente pela diversão e pelo prazer de provar que eles podem fazer isso. Eles não roubam nada, não ganham dinheiro com suas explorações. Não destroem nenhum arquivo, não interrompem as conexões de rede nem paralisam nenhum sistema de computadores. O simples fato de eles estarem lá pegando cópias de arquivos e pesquisando as mensagens de correio eletrônico em busca das senhas e de fazer isso pelas costas da segurança e dos administradores de rede torce os narizes das pessoas que são responsáveis por afastar os intrusos como eles. Grande parte da satisfação está no fato de fazerem isso sozinhos.

Fiel ao seu perfil, o nosso Danny queria examinar os detalhes do produto mais guardado da sua empresa-alvo só para satisfazer a sua própria curiosidade e admirar as inovações que o fabricante estava para lançar.

Nem é preciso dizer que os projetos de produto eram segredos comerciais cuidadosamente guardados, tão preciosos e protegidos quanto qualquer outra coisa que a empresa possuía. Danny sabia disso. E não ligava nem um pouco. Afinal de contas, essa era apenas uma empresa grande e sem nome.

Mas como obter o código-fonte do software? Acontece que se apoderar das jóias da coroa do Grupo de Comunicações Seguras da empresa acabou sendo uma coisa muito fácil, muito embora a empresa fosse uma daquelas que usavam a *autenticação de dois fatores*, um método no qual as pessoas devem usar não um, mas dois identificadores separados para provar suas identidades.

Este é um exemplo que talvez você já conhece. Quando chega a renovação do seu cartão de crédito, você tem de ligar para a administradora para informar que o cartão está nas mãos do cliente certo, e não nas mãos de alguém que roubou o envelope do correio. As instruções que vêm com o cartão hoje em dia geralmente dizem para você ligar de casa. Quando você liga, o software da administradora do

Jargão

AUTENTICAÇÃO DE DOIS FATORES **O uso de dois tipos diferentes de autenticação para verificar a identidade. Por exemplo, uma pessoa pode ter de identificar a si mesma ligando de uma determinada localização identificável e sabendo uma senha.**

cartão analisa a *ANI,* a identificação de número automática, a qual é fornecida pelo atendimento das ligações que são pagas pela empresa do cartão de crédito.

Um computador da administradora do cartão usa o número do cliente que está ligando fornecido pela ANI e compara esse número com o banco de dados de titulares de cartão da empresa. Quando o operador entra na linha, a sua tela exibe as informações do banco de dados com os detalhes do cliente. Assim sendo, o operador já sabe que a ligação está sendo feita da casa de um cliente e essa é uma forma de autenticação.

O operador escolhe um item nas informações exibidas sobre você — quase sempre o número do seguro social, a data de nascimento ou o nome de solteira da mãe — e pede que você repita essas informações. Se você fornecer a resposta certa, essa é uma segunda forma de autenticação — com base nas informações que você deve saber.

Na empresa que fabrica os sistemas de rádio de segurança da nossa história, cada empregado que tem acesso ao computador tinha o seu nome normal de conta e a sua senha. Entretanto, além disso. ele recebia um pequeno dispositivo eletrônico chamado ID Seguro projetado em tecnologias *one-time password.* Isso é aquilo que é chamado de token baseado em tempo. Esses dispositivos são de dois tipos: um tem cerca de metade do tamanho de um cartão de crédito, mas um pouco mais fino; o outro é pequeno o bastante para que as pessoas possam colocá-lo em seus chaveiros.

Tirado do mundo da criptografia, esse dispositivo em particular tem uma pequena janela que exibe uma série de seis dígitos. A cada 60 segundos, o vídeo muda e mostra um número de seis dígitos diferente. Quando uma pessoa autorizada precisa de acesso externo à rede, ela primeiro precisa se identificar como um usuário autorizado digitando o seu código secreto e os dígitos exibidos no seu dispositivo. Após a verificação do sistema interno, ela é autenticada com o seu nome de conta e senha.

Para o jovem hacker Danny chegar até o código-fonte que tanto cobiçava, ele teria não apenas de fornecer o nome de conta e a senha de algum empregado (um desafio não muito grande para o experiente engenheiro social), mas também teria de contornar o problema do token baseado em tempo.

Burlar a autenticação de dois fatores de um token baseado em tempo combinado a um código de identificação secreta do usuário parece um desafio tirado do filme *Missão Impossível.* Mas para os engenheiros sociais, o desafio é semelhante àquele enfrentado por um jogador de pôquer que tem uma habilidade além do normal para fazer uma leitura dos seus oponentes. Com um pouco de sorte, quando se senta em uma mesa, ele sabe que vai sair dali com uma pilha grande de dinheiro alheio.

A investida contra o forte

Danny começou fazendo a lição de casa. Em pouco tempo ele havia conseguido juntar informações suficientes para se fazer passar por um verdadeiro empregado. Ele tinha um nome de empregado, o departamento, o número do telefone e o número do empregado, bem como o nome e telefone do gerente.

Agora era a calmaria antes da tempestade. Literalmente. Seguindo o plano que havia estabelecido, Danny precisava de mais uma coisa antes da próxima etapa, e isso era algo sobre o qual não tinha nenhum controle: ele precisava de uma tempestade de neve. Danny precisava de um pouco de ajuda de São Pedro na forma de um tempo tão ruim que os empregados não conseguiriam chegar ao escritório.

No inverno de Dakota do Sul, onde está localizada a fábrica em questão, todos que esperavam mau tempo não tinham de esperar muito. Na sexta-feira à noite, a tempestade chegou. Aquilo que começou como neve rapidamente se transformou em chuva congelante, e de manhã as estradas estavam cobertas de uma camada grossa e perigosa de gelo. Para Danny essa era a oportunidade perfeita.

Ele ligou para a fábrica, pediu para falar com a sala de computadores e falou com uma das abelhas operárias de TI, um operador de computador que se apresentou como Roger Kowalski.

Dando o nome do empregado real que havia obtido, Danny disse: "Aqui é Bob Billings. Trabalho no Grupo de Comunicações Seguras. Estou em casa e não posso chegar ao trabalho por causa da tempestade. E o problema é que preciso acessar a minha estação de trabalho e o meu servidor daqui de casa e deixei o meu ID Seguro na minha mesa. Você pode procurá-lo para mim? Ou alguém pode fazer isso? E, depois, você pode ler o meu código quando eu precisar dele? A minha equipe tem um prazo crítico e não há como eu terminar o trabalho. E não há como chegar ao escritório — as estradas estão muito perigosas por aqui."

O operador do computador respondeu: "Não posso sair do Centro de Computadores."

Danny respondeu rapidamente: "Você tem um ID Seguro?"

"Há um aqui no Centro de Computadores", ele disse. "Nós o reservamos para os operadores em caso de emergência."

"Ouça", disse Danny. "Você pode me fazer um grande favor? Quando eu precisar discar para a rede, você pode me emprestar o seu ID Seguro? Só até que seja seguro dirigir até aí".

"Quem e você mesmo?", Kowalski perguntou.

"Bob Billings."

"Para quem você trabalha?"

"Para Ed Trenton."

"Ah, sim. Eu o conheço."

Quando há chances de enfrentar condições muito desfavoráveis, um bom engenheiro social faz mais do que a pesquisa normal. "Estou no segundo andar", continuou Danny. "Perto do Roy Tucker."

O operador também conhecia aquele nome. Danny voltou a trabalhar com ele. "Seria muito mais fácil se você fosse até a minha mesa e conseguisse o ID Seguro para mim."

Danny tinha certeza de que o rapaz não entraria nessa. Antes de mais nada, ele não ia querer sair no meio do seu turno, percorrer corredores, subir escadas para chegar até algum lugar distante do prédio. Ele também não ia querer colocar as mãos na mesa de outra pessoa, violando o espaço pessoal de alguém. Não, com quase toda a certeza ele não ia querer fazer isso.

Kowalski não queria dizer não para um colega de trabalho que precisava de ajuda, mas também não queria dizer sim e ter problemas. Assim sendo, passou a decisão para outro: "Terei de falar com o meu chefe. Aguarde um pouco." Ele colocou o telefone na mesa e Danny o ouviu pegar outro telefone. fazer a ligação e explicar a solicitação. Em seguida, Kowalski fez algo inexplicável: ele endossou a história do homem que usava o nome de Bob Billings. "Eu o conheço", ele disse ao gerente. "Ele trabalha com Ed Trenton. Podemos deixá-lo usar o ID Seguro do Centro de Computadores?" Danny,

segurando o telefone, ficou surpreso ao ouvir esse apoio extraordinário e inesperado à sua causa. Ele não acreditava no que estava ouvindo ou em sua sorte.

Após alguns momentos, Kowalski voltou ao telefone: "O meu gerente quer falar com você." Deu-lhe o nome do homem e o número do seu celular.

Danny ligou para o gerente e contou toda a história de novo, incluindo detalhes sobre o projeto no qual estava trabalhando e o motivo pelo qual a sua equipe de produto precisava cumprir um prazo crítico. "Seria mais fácil se alguém fosse lá e pegasse o meu cartão", ele reafirmou. "Acho que a mesa não está trancada e o cartão deve estar na minha gaveta esquerda superior."

"Bem", entabulou o gerente, "só pelo final de semana, acho que podemos deixá-lo usar o cartão do Centro de Computadores. Vou falar para quem estiver de serviço que quando você ligar, eles devem ler o código de acesso aleatório para você". Ele lhe deu o número de identificação a ser usado com o cartão.

Durante todo o final de semana, sempre que Danny queria entrar no sistema corporativo de computadores, só tinha de ligar para o Centro de Computadores e pedir para eles lerem os seis dígitos exibidos no token de ID Seguro.

Um trabalho interno

Depois de estar dentro do sistema de computadores da empresa, o que aconteceu? Como Danny encontraria o servidor que tinha o software que desejava?

Ele já estava preparado para isso.

Muitos usuários de computadores conhecem os newsgroups, aquele conjunto grande de bulletin boards eletrônicos nos quais as pessoas podem publicar perguntas para que outras pessoas respondam, ou podem encontrar companheiros virtuais que compartilham do interesse em música, computadores ou em centenas de outros assuntos.

O que poucas pessoas sabem quando postam uma mensagem em um site de newsgroup é que elas permanecem on-line e disponíveis por anos a fio. O Google, por exemplo, já mantém um arquivo de 700 milhões de mensagens, sendo que algumas delas datam de 20 anos atrás! Danny começou a entrar no endereço na Web http://groups.google.com.

Como termos da pesquisa Danny inseriu "criptografia de comunicações por rádio" e o nome da empresa e encontrou uma mensagem com alguns anos de idade sobre o assunto de um empregado. Era uma publicação que havia sido feita quando a empresa estava começando a desenvolver o produto, provavelmente muito antes de os departamentos de polícia e dos órgãos federais pensarem em misturar os sinais de rádio.

A mensagem contida na assinatura do remetente dava não apenas o nome do homem, Scott Baker, mas também o número do seu telefone e até mesmo o nome do seu grupo de trabalho, o Grupo de Comunicações Seguras.

Danny pegou o telefone e discou o número. Já fazia muito tempo — será que ele ainda estava trabalhando na mesma organização anos depois? Ele estaria trabalhando em um final de semana com aquela tempestade? O telefone tocou uma, duas, três vezes e depois Scott atendeu.

Dizendo ser do Departamento de TI da empresa. Danny convenceu Baker (usando uma das maneiras que agora você já conhece dos capítulos anteriores) a revelar os nomes dos servidores usados para o trabalho de desenvolvimento. Esses eram os servidores nos quais poderia estar o código-fonte com o algoritmo de criptografia proprietário e o firmware usados nos produtos de rádio de segurança da empresa.

Danny estava cada vez mais próximo e o seu entusiasmo aumentava. Ele estava prevendo a satisfação, a sensação ótima que ele tinha quando conseguia fazer algo que sabia que apenas um número limitado de pessoas poderia realizar.

Mesmo assim, ele ainda não estava seguro. No restante do final de semana ele poderia entrar na rede da empresa sempre que quisesse, graças àquele prestativo gerente do centro de computadores. E sabia quais servidores queria acessar. Mas quando discou, o servidor de terminal ao qual se conectou não permitiu que ele se conectasse aos sistemas de desenvolvimento do Grupo de Comunicações Seguras. Deveria haver um firewall interno ou um roteador que protegia os sistemas de computadores daquele grupo. Ele teria de encontrar algum outro modo de entrar.

A próxima etapa exigiu sangue frio. Danny ligou de novo para Kowalski no departamento de Operações de Computador e reclamou: "O meu servidor não me permite conectar", e disse ao funcionário de TI: "Preciso configurar uma conta em um dos computadores do seu departamento para poder usar a Telnet e me conectar ao meu sistema."

O gerente já havia aprovado a divulgação do código de acesso exibido no token baseado em tempo, de modo que esta nova solicitação não parecia exagerada. Kowalski configurou uma conta e senha temporária em um dos computadores do Centro de Operações e pediu a Danny: "Ligue de volta quando não precisar mais dela para eu removê-la."

Após fazer o login na conta temporária, Danny conseguiu se conectar à rede dos sistemas de computadores do Grupo de Comunicações Seguras. Depois de uma hora pesquisando on-line uma vulnerabilidade técnica que lhe desse acesso ao servidor principal de desenvolvimento ele conseguiu. Aparentemente, o sistema ou o administrador da rede não estavam atentos às últimas comunicações sobre bugs de segurança no sistema operacional que permitia o acesso remoto. Mas Danny estava.

Em pouco tempo ele localizou os arquivos de código-fonte que procurava e os transferiu remotamente para um site de comércio eletrônico que oferecia espaço grátis de armazenamento. Nesse site, mesmo que os arquivos fossem descobertos, não seria possível rastrear para descobrir quem os enviou.

Ele tinha de executar uma última etapa antes de se desconectar: o processo metódico de apagar suas pegadas. Ele terminou antes do programa de televisão sair do ar naquela noite. Danny calculou que esse havia sido um bom trabalho de final de semana. E não teve de se arriscar pessoalmente. Isso foi muito emocionante, melhor ainda do que a adrenalina de praticar snowboarding ou pára-quedismo.

Danny ficou bêbado aquela noite, não com scotch, gim, cerveja ou saque, mas no sentido do poder e da realização à medida que despejava os arquivos que havia roubado, fechando com a ilusão do software de rádio secretíssimo.

Analisando a trapaça

Como na história anterior, este golpe só funcionou porque um empregado da empresa estava disposto a aceitar o fato de que um interlocutor era realmente o empregado que alegava ser. Por sua vez, essa disposição de ajudar um colega com um problema faz parte daquilo que lubrifica as engrenagens da indústria, e parte daquilo que torna os empregados de algumas empresas mais agradáveis de trabalhar do que os empregados de outras empresas. Mas essa disposição em ajudar pode ser uma grande vulnerabilidade que um engenheiro social tentará explorar.

Um tipo de truque que Danny usou era delicioso: quando solicitou que alguém pegasse o seu ID Seguro na sua mesa, ele pediu que alguém "pegasse" para ele. Pegar é uma ordem que você dá para

o seu cachorro. Ninguém quer receber a ordem de pegar alguma coisa. Com aquela única palavra, Danny garantiu que a solicitação seria recusada e que alguma outra solução seria aceita, o que era exatamente aquilo que desejava.

O operador do Centro de Computadores, Kowalski, foi convencido pelo fato de Danny falar nomes de pessoas que ele conhecia. Mas por que o *gerente* — nada menos do que um gerente de TI — permite que um estranho acesse a rede interna da empresa? Simplesmente porque a ligação pedindo ajuda pode ser uma ferramenta poderosa e persuasiva do arsenal do engenheiro social.

Recado do Mitnick

Esta história mostra que os tokens baseados em tempo e outras formas semelhantes de autenticação não são defesa contra o astuto engenheiro social. A única defesa é um empregado consciente que segue as políticas de segurança e entende como as outras pessoas podem influenciar de modo malicioso o seu comportamento.

Algo assim poderia acontecer na *sua* empresa? Isso já aconteceu?

EVITANDO A TRAPAÇA

Um elemento que parece se repetir sempre nessas histórias é o fato de um atacante conseguir discar para uma rede de computadores de fora da empresa, sem que a pessoa que o ajuda tome as devidas precauções para verificar se ele é realmente um empregado e pode ter o acesso. Por que volto com tanta freqüência a esse mesmo tema? Porque esse é um fator importante de tantos ataques da engenharia social. Para o engenheiro social, essa e a maneira mais fácil de atingir o seu objetivo. Por que um atacante gastaria horas tentando fazer a invasão, quando pode fazer isso com uma simples ligação telefônica?

Um dos métodos mais poderosos pelo qual o engenheiro social pode executar esse tipo de ataque é usar o golpe simples de fingir que precisa de ajuda — uma abordagem muito usada pelos atacantes. Você não vai querer fazer com que os seus empregados parem de cooperar com colegas ou clientes e, assim, precisa fornecer-lhes procedimentos de verificação específicos a serem usados com todos que façam uma solicitação de acesso ao computador ou a informações confidenciais. Dessa forma, eles podem ser úteis para aqueles que merecem a ajuda, e ao mesmo tempo podem proteger os ativos de informação da organização e os sistemas de computadores.

Os procedimentos de segurança da empresa precisam declarar com detalhes o tipo de mecanismo de verificação que deve ser usado nas diversas circunstâncias. O Capítulo 17 fornece uma lista de procedimentos detalhada, mas estas são algumas orientações que devem ser levadas em conta:

- Uma boa forma de verificar a identidade de uma pessoa que faz uma solicitação é ligar para o número de telefone relacionado na lista de telefones da empresa para aquela pessoa. Se a pessoa que faz a solicitação for realmente um atacante, a ligação de verificação permitirá que você fale com a pessoa verdadeira ao telefone enquanto o impostor aguarda na linha, ou permite que você ouça o som da voz da pessoa no voice mail para poder compará-lo com a voz do atacante.
- Se forem usados números de empregados na sua empresa para verificar a identidade, esses números têm de ser tratados como informações confidenciais, guardados cuidadosamente e

não podem ser dados a estranhos. O mesmo vale para todos os outros tipos de identificadores internos, tais como números de telefone, identificadores de faturamento de departamentos e até mesmo os endereços de correio eletrônico.

- O treinamento corporativo deve chamar a atenção de todos para a prática comum de aceitar pessoas desconhecidas como empregados legítimos, com base no fato de que eles parecem ter autoridade ou conhecimento. Só porque alguém conhece a prática de uma empresa ou usa a terminologia interna, não há motivos para assumir que a sua identidade não precisa ser verificada de outras maneiras.
- Os encarregados da segurança e os administradores de sistemas precisam sempre prestar atenção ao modo como *iodas* as pessoas têm consciência da segurança. Eles também precisam ter certeza de que eles próprios estão seguindo as mesmas regras, procedimentos e práticas.
- As senhas e outros itens semelhantes, obviamente, nunca devem ser compartilhados, mas a restrição contra o compartilhamento é mais importante ainda no caso dos tokens baseados em tempo e em outras formas seguras de autenticação. É uma questão de bom senso o fato de que o compartilhamento de um desses itens vai contra o motivo pelo qual a empresa instalou os sistemas. O compartilhamento significa que não pode haver responsabilidade. Se um incidente de segurança ocorre ou se algo de errado acontece, você não poderá determinar quem é o responsável.
- Como reitero neste livro, os empregados precisam estar familiarizados com as estratégias da engenharia social e seus métodos para analisar com responsabilidade as solicitações recebidas. Considere o uso da dramatização como parte do treinamento em segurança, para que os empregados possam entender melhor como o engenheiro social age.

Capítulo 7

Sites Falsos e Anexos Perigosos

Há um velho ditado que diz que você nunca tem nada de graça. Mesmo assim, o golpe de oferecer algo de graça continua sendo uma grande jogada de negócios legítimos ("Mas não é só isso! Ligue agora mesmo e ganhe um conjunto de facas e uma pipoqueira!") e não tão legítimos ("Compre um acre de pântanos na Flórida e ganhe um segundo acre de graça!").

E a maioria de nós gosta tanto de ganhar algo de graça que pode se enganar e não pensar com clareza na oferta ou na promessa que está sendo feita. Conhecemos o aviso "cuidado ao comprar", mas está na hora de prestar atenção em outro aviso: cuidado com os anexos que vêm nas mensagens de correio eletrônico e com o software grátis. O atacante experiente usa quase que qualquer meio para invadir a rede corporativa, incluindo o apelo para o nosso desejo natural de receber um presente grátis. Estes são alguns exemplos.

"VOCÊ GOSTARIA DE GANHAR UM (ESPAÇO EM BRANCO) GRÁTIS?"

Assim com as viroses têm sido uma praga para a humanidade e os médicos desde o início dos tempos, os vírus de computadores também representam uma praga para os usuários da tecnologia. Aqueles que chamam mais a atenção e têm mais projeção, não por acaso, causam os maiores danos. Eles são o produto dos vândalos dos computadores.

Como feras dos computadores que se transformaram em malucos maliciosos, esses vândalos lutam para mostrar como são inteligentes. Eventualmente seus atos são como um ritual de iniciação, destinados a impressionar os hackers mais velhos e mais experientes. Essas pessoas são motivadas para criar um worm ou um vírus para infligir um dano. Se o seu trabalho destruir arquivos, acabar com unidades de disco inteiras e seguir por correio eletrônico para milhares de pessoas desavisadas, os vândalos alardeiam com orgulho sua realização. Se os vírus causarem um caos suficiente para aparecerem nos jornais e as notícias da rede avisarem contra eles, melhor ainda.

Muito foi escrito sobre os vândalos e seus vírus. Livros, programas de software e empresas inteiras surgiram para oferecer proteção, e não falaremos aqui das defesas contra seus ataques técnicos. O nosso interesse no momento focaliza menos os atos destrutivos do vândalo do que os esforços mais concentrados do seu primo distante: o engenheiro social.

Chegou no correio eletrônico

Todos os dias você recebe mensagens de correio eletrônico com propaganda ou oferecendo alguma coisa de que não precisa e não quer. Você sabe como é. Eles prometem consultoria de investimentos,

descontos em computadores, televisões, câmeras, vitaminas ou viagens, oferecem cartões de crédito de que não precisa, um dispositivo que permite receber os canais da televisão paga de graça, maneiras de melhorar a sua saúde ou a sua vida sexual e assim por diante.

Mas de vez em quando uma oferta aparece na sua caixa de correio eletrônico, uma oferta que chama a sua atenção. Isso pode ser um jogo de graça, uma oferta de fotos do seu astro preferido, um programa de agenda grátis ou um shareware barato que protege o seu computador contra vírus. Independente de qual seja a oferta, a mensagem direciona você para fazer o download do arquivo com os bens que a mensagem o convenceu a experimentar.

Você também pode receber uma mensagem com uma linha de assunto dizendo "Não perca" ou Ana, por que você não escreveu para mim?" ou "Oi, Tim, esta é a foto sexy que eu prometi para você". Isso não pode ser mala direta de propaganda, você pensa, porque tem o seu nome e parece tão pessoal. Assim sendo, abre o anexo para ver a foto ou ler a mensagem.

Todas essas ações — fazer o download de software que você conheceu em uma mensagem de propaganda, clicar em um link que o leva até um site do qual nunca ouviu falar antes, abrir um anexo de alguém que não conhece — são convites para problemas. Com certeza, na maior parte do tempo aquilo que você tem é exatamente aquilo que esperava, ou na pior das hipóteses algo decepcionante ou ofensivo, mas inofensivo. Mas, eventualmente, você recebe o trabalho de um vândalo.

O envio de código malicioso para o seu computador *é* apenas uma pequena parte do ataque. O atacante precisa convencê-lo a fazer o download do anexo para que o ataque seja bem-sucedido.

As formas mais perigosas de código malicioso — worms com nomes tais como Love Letter, SirCam e Anna Kournikova, só para mencionar alguns — aproveitam-se das técnicas da engenharia social que fraudam e exploram o seu desejo de obter algo de graça para se espalharem. O worm chega como um anexo de uma mensagem de correio eletrônico que oferece algo tentador, tal como informações confidenciais, pornografia grátis ou — um truque mais inteligente — uma mensagem dizendo que o anexo é o recibo de algum item caro que você deve ter comprado. Este último golpe leva você a abrir o anexo com medo de o seu cartão de crédito ter sido usado para o débito de um item que não queria.

É impressionante o número de pessoas que caem nesses truques; mesmo após saberem sobre os perigos de abrirem anexos de correio eletrônico, a consciência do perigo passa com o tempo e nos deixa vulneráveis.

Detectando o software malicioso

Outro tipo de *malware* -- abreviação de *malicious software* — coloca no seu computador um programa que opera sem o seu conhecimento ou consentimento ou que executa uma tarefa sem que você saiba. O malware pode parecer inocente, talvez um documento do Word ou uma apresentação do PowerPoint, ou qualquer programa que tenha a funcionalidade das macros, mas ele instala secretamente um programa não autorizado. Por exemplo, o malware pode ser uma versão do Cavalo de Tróia de que falamos

Observação

Um tipo de programa conhecido no submundo dos computadores como *RAT* ou *Remote Access Trojan* dá ao atacante o acesso total ao seu computador, como se ele estivesse sentado no seu teclado!

Jargão

MALWARE Gíria para o software malicioso, um programa de computador, tal como um vírus, um worm ou um Cavalo de Tróia, que executa tarefas prejudiciais.

no Capítulo 6. Após esse software ser instalado na sua máquina, ele pode transmitir para o atacante cada tecla que você digita, incluindo todas as suas senhas e números de cartões de crédito.

Existem outros dois tipos de software malicioso que você vai achar chocantes. Um deles pode passar para o atacante cada palavra que você falar dentro do âmbito do microfone do seu computador, *mesmo quando você acha que o microfone está desligado.* Pior ainda, se você tiver uma Web cam instalada no seu computador, um atacante que use uma variação dessa técnica pode capturar tudo que ocorre na frente do seu terminal, mesmo quando você acha que a câmera está desligada, seja dia ou noite.

Recado do Mitnick

Cuidado com os malucos que oferecem presentes, caso contrário a sua empresa pode ter a mesma sorte da cidade de Tróia. Quando tiver dúvidas e para evitar uma infecção, use proteção.

Um hacker com um senso de humor malicioso pode tentar plantar no seu computador um pequeno programa criado para aborrecer. Por exemplo, ele pode fazer com que a sua unidade de CD-ROM fique abrindo sem parar, ou que o arquivo no qual você está trabalhando seja minimizado. Ou então, ele pode fazer com que um arquivo de áudio reproduza um grito no volume mais alto no meio da noite. Nada disso é muito engraçado quando você está tentando dormir ou trabalhar, mas pelo menos eles não causam nenhum dano duradouro.

MENSAGEM DE UM AMIGO

Os cenários podem ficar ainda piores, apesar das suas precauções. Imagine que você resolveu não correr riscos. Você não vai mais descarregar nenhum arquivo, exceto de sites seguros que conhece e confia, tais como o SecurityFocus.com ou o Amazon.com. Você não clica mais nos links de correio eletrônico de fontes desconhecidas. Você não abre mais os anexos de nenhuma mensagem que não estava esperando. E verifica a sua página de browser para ter certeza de que há um símbolo de site seguro em cada site que visita para realizar transações de comércio eletrônico ou para trocar informações confidenciais.

Então, um belo dia você recebe uma mensagem de correio eletrônico de um amigo ou empresa associada que tem um anexo. Não poderia ser algo malicioso, já que vem de alguém que você conhece, não é mesmo? Particularmente porque sabe a quem culpar se os dados do seu computador forem danificados.

Você abre o anexo e... BOOM! Acabou de receber um Cavalo de Tróia. Por que alguém que você conhece faria isso? Porque algumas coisas não são o que parecem ser. Você já leu sobre isso: o worm

que entra no computador de alguém e depois envia mensagens de correio eletrônico ele mesmo para todas as pessoas do seu catálogo de endereços. Cada uma daquelas pessoas recebe uma mensagem de correio eletrônico de alguém que conhece e confia, e cada uma daquelas mensagens de correio eletrônico de confiança contém o worm, o qual se propaga como as ondas formadas por uma pedra jogada em um lago tranqüilo.

O motivo da eficiência dessa técnica é que ela segue a teoria de matar dois coelhos com uma só cajadada. A capacidade de propagar-se para as outras vitimas desavisadas e a aparência de que veio de uma pessoa de confiança.

Recado do Mitnick

O homem inventou muitas coisas maravilhosas que mudaram o mundo e a nossa forma de viver. Mas para cada bom uso da tecnologia, o computador, o telefone ou a Internet, alguém sempre encontra um modo de abusar dessa tecnologia em proveito próprio.

O triste fato é que no estado atual da tecnologia você pode receber uma mensagem de correio eletrônico de alguém próximo e ter de se perguntar se é seguro abri-la.

VARIAÇÕES SOBRE UM MESMO TEMA

Nesta era da Internet, há um tipo de fraude que envolve o seu redirecionamento para um site Web que não é aquele que você esperava. Isso acontece regularmente e assume várias formas. Este exemplo, que se baseia em um golpe real executado na Internet, é representativo.

Feliz Natal...

Um vendedor de seguros aposentado chamado Edgar recebeu uma mensagem de correio eletrônico certo dia da PayPal, uma empresa que oferece um modo rápido e conveniente de fazer pagamentos on-line. Esse tipo de serviço é muito útil quando uma pessoa de uma parte do pais (ou do mundo) está comprando um item de um indivíduo que ele não conhece. A PayPal cobra no cartão de crédito do comprador e transfere o dinheiro diretamente para a conta do vendedor.

Como colecionador de vasos antigos de vidro, Edgar fez muitos negócios por meio da empresa de leilões on-line eBay. Ele usava a PayPal com freqüência várias vezes por semana. Assim sendo. Edgar ficou interessado quando recebeu uma mensagem de correio eletrônico nas festas de fim de ano de 2001, a qual parecia vir da PayPal e oferecia um prêmio pela atualização da sua conta com a PayPal. A mensagem dizia:

> Boas Festas caro cliente PayPal;
>
> À medida que o Ano Novo se aproxima e todos nos preparamos para iniciar um novo ano, a PayPal gostaria de lhe dar um crédito de US$ 5 na sua conta!
>
> Tudo que você precisa fazer para receber os seus US$ 5,00 de presente é atualizar as suas informações no nosso site seguro Pay Pal até 1º de janeiro de 2002. Um ano traz muitas chances, e atualizando as suas informações conosco, você permitirá que continuemos a lhe fornecer nosso valioso serviço ao cliente com excelente qualidade e. além de tudo, você estará mantendo os nossos registros atualizados!

Para atualizar as suas informações agora e receber os US$ 5,00 na sua conta da PayPal instantaneamente, clique neste link:

http://www.paypal-secure.com/cgi-bin

Obrigado por usar a PayPal.com e nos ajudar a crescer e sermos os maiores da nossa área!

Desejando-lhe sinceramente um "Feliz Natal e Ano Novo",

Equipe da PayPal

Uma observação sobre os sites Web de comércio eletrônico

Provavelmente você conhece pessoas que não gostam de comprar coisas on-line, mesmo de empresas de nome como Amazon e eBay, ou em sites Web da Old Navy, Target ou Nike. De certa forma, eles estão certos em desconfiar. Se o seu browser usa a criptografia de 128 bits. que é o padrão atual, as informações que envia para qualquer site seguro saem criptografadas do seu computador. Esses dados podem ser decriptografados com muito esforço, mas provavelmente isso não pode ser feito dentro de um prazo razoável, exceto talvez pela National Security Agency (e a NSA, até onde sabemos, não mostrou nenhum interesse em roubar números de cartões de crédito de cidadãos americanos, nem tenta descobrir quem está pedindo vídeos de sexo ou lingerie de sex shop).

Esses arquivos criptografados poderiam ser quebrados por qualquer pessoa que tivesse tempo e recursos. Mas, na verdade, quem seria bobo de ter todo esse trabalho para roubar *um* número de cartão de crédito, quando muitas empresas de comércio eletrônico cometem o erro de armazenar todas as informações financeiras de seus clientes decriptografadas em seus bancos de dados? Pior ainda, diversas empresas de comércio eletrônico que usam um determinado banco de dados SQL agravam ainda mais esse problema: elas nunca mudaram a senha default do administrador de sistema para o programa. Quando tiraram o programa da caixa, a senha era "null" e ainda é "null" hoje. Assim sendo, o conteúdo dos bancos de dados está disponível para todos na Internet que resolvem tentar se conectar ao servidor do banco de dados. Esses sites estão sob ataque o tempo todo e as informações são roubadas, sem que ninguém lenha culpa.

Por sua vez. as mesmas pessoas que não compram na Internet porque têm medo de ter suas informações de cartão de crédito roubadas não têm problemas em comprar com aquele mesmo cartão de crédito em uma loja de material de construção ou pagar o almoço, jantar ou drinques com o cartão — mesmo em um bar de uma rua deserta ou no restaurante no qual não levariam suas mães. Os recibos dos cartões de crédito são roubados desses locais o tempo todo, ou pescados nas latas de lixo da rua de trás. E todo caixa ou garçom inescrupuloso pode anotar as suas informações de nome e cartão ou podem usar um dispositivo facilmente disponível na Internet, um dispositivo de varredura, que armazena os dados de qualquer cartão de crédito que é passado por ele para recuperação posterior.

Existem alguns perigos na compra on-line, mas provavelmente ela é mais segura do que comprar em uma loja de material de construção. E as empresas de cartão de crédito oferecem a mesma proteção quando você usa o seu cartão on-line — se alguma taxa fraudulenta for cobrada da conta, você só é responsável pelos primeiros US$ 50,00.

Assim sendo, na minha opinião, o medo da compra on-line é apenas outra preocupação injustificada.

Edgar não notou nenhum dos sinais conhecidos de que havia algo de errado com o seu correio eletrônico (por exemplo, o ponto-e-vírgula depois da linha de cumprimentos e o texto enrolado sobre "nosso valioso serviço ao cliente com excelente qualidade"). Ele clicou no link, inseriu as informações solicitadas — nome, endereço, número do telefone e as informações do cartão de crédito — e aguardou que o crédito de US$ 5,00 aparecesse na sua próxima fatura do cartão de crédito. Entretanto, o que apareceu foi uma lista de taxas pelos itens que nunca comprou.

Analisando a trapaça

Edgar foi pego por um golpe comum na Internet. Esse é um golpe que chega de diversas maneiras. Uma delas (detalhada no Capítulo 9) envolve uma tela de login falsa criada pelo atacante, a qual é idêntica à tela real. A diferença é que a tela falsa não dá acesso ao sistema de computadores que o usuário está tentando atingir, mas sim passa o seu nome de usuário e a senha para o hacker

Edgar foi pego em um golpe no qual os bandidos registraram um site Web com o nome "paypal-secure.com" — o qual parece como se fosse uma página segura do site legítimo da PayPal, mas não e. Quando ele inseriu as informações naquele site, os atacantes conseguiram o que queriam.

Recado do Mitnick

Embora isso não seja infalível (e nenhuma segurança é), sempre que visitar um site que solicita informações que você considera confidenciais, verifique se a conexão está autenticada e criptografada. E o mais importante, não clique automaticamente em Sim em nenhuma caixa de diálogo que possa indicar uma questão de segurança, tal como um certificado digital inválido, vencido ou revogado.

VARIAÇÕES SOBRE A VARIAÇÃO

Quantas outras maneiras existem de enganar os usuários de computador para que eles entrem em um site Web falso no qual têm de fornecer informações confidenciais? Não suponho que alguém tenha uma resposta válida e precisa, mas "muitas e muitas" servirão para essa finalidade.

O elo que falta

Um truque surge regularmente: o envio de uma mensagem de correio eletrônico que oferece um motivo tentador para visitar um site e fornece um link para ir diretamente a ele. Só que o link não leva você ao site que acha que está indo, porque ele na verdade apenas se parece com um link daquele site. Este é outro exemplo que na verdade foi usado na Internet envolvendo novamente o mal uso do nome da PayPal:

www.PayPai.com

Olhando rapidamente, parece que diz PayPal. Mesmo se a vítima notar, ela pode achar que é apenas um erro no texto que faz com que o "l" de Pal se pareça com um "i". E quem notaria de relance que este endereço

www.PayPa1.com

msg: Caro usuário da eBay,

Ficou claro que alguém corrompeu a sua conta na eBay e violou a política abaixo do nosso Contrato de Usuário:

4. Lances e compra

Você é obrigado a concluir a transação com o vendedor se comprar um item por meio dos nossos formatos fixos de preço ou tiver o lance maior descrito abaixo. Se der o maior lance no final de um leilão (atendendo o mínimo aplicável ou os requisitos de reserva) e o seu lance for aceito pelo vendedor, você é obrigado a concluir a transação com o vendedor, ou a transação é proibida por lei ou por este Contrato.

Você recebeu este aviso da eBay porque veio ao nosso conhecimento que a sua conta corrente causou interrupções nos outros membros da eBay e a eBay exige a verificação imediata da sua conta. Por favor, verifique a sua conta, caso contrário ela será desativada. Clique Aqui para Verificar a Sua Conta — http://error_ebay.tripod.com

As marcas designadas são de propriedade de seus respectivos proprietários eBay e o logotipo da eBay são marcas registradas da eBay Inc.

Figura 7.1 Um link deste tipo e de outras mensagens de correio eletrônico deve ser usado com cautela.

usa o número 1 no lugar da letra L minúscula? Há um número suficiente de pessoas que aceitam os erros de digitação e outros probleminhas que tornam esse truque cada vez mais usado pelos bandidos dos cartões de crédito. Quando as pessoas entram em um site falso, ele se parece com o site que elas esperam ver, e inserem as informações do seu cartão de crédito. Para criar um desses golpes, um atacante só precisa registrar o nome do domínio falso, enviar as mensagens de correio eletrônico e aguardar que os trouxas apareçam, prontos para serem enganados.

Na metade do ano de 2002, recebi uma mensagem de correio eletrônico aparentemente como parte de uma mala direta que era marcada como sendo da "Ebay@ebay.com". A mensagem é mostrada na Figura 7.1.

As vítimas que clicaram no link foram para uma página da Web muito parecida com uma página da eBay. Na verdade, a página era bem feita, com o logotipo eBay autêntico e com os links "Browse", "Sell" e outros links de navegação, os quais, quando clicados, levavam o visitante ao site real da eBay. Havia também um logotipo de segurança no canto direito inferior. Para distrair a vítima experiente, o criador usou até mesmo a criptografia HTML para mascarar o lugar onde iam as informações fornecidas pelo usuário.

Esse foi um exemplo excelente de um ataque malicioso da engenharia social baseado em computador. Mesmo assim, ele ainda tinha várias falhas.

A mensagem de correio eletrônico não estava bem escrita. Em particular, o parágrafo que começava com "Você recebeu este aviso" é confusa e inadequada (a pessoa responsável por esses boatos

Observação

Por que as pessoas podem registrar nomes de domínio fraudulentos ou inapropriados? Porque na lei atual e na política on-line todos podem registrar qualquer nome de site que ainda não seja usado.

As empresas tentam combater esse uso da imitação de endereços, mas pense no que enfrentam. A General Motors processou uma empresa que registrou fkgeneralmotors.com (mas sem os asteriscos) e apontou o URL para o site Web da General Motors. A GM perdeu.**

nunca contrata um profissional para editar o texto e os erros sempre aparecem). Da mesma forma, alguém que esteja prestando atenção suspeita do fato de a eBay pedir as informações da PayPal do visitante; não há motivo para a eBay pedir as informações particulares de um cliente envolvendo uma empresa diferente.

Uma pessoa com conhecimento da Internet provavelmente reconheceria que o hiperlink se conecta não ao domínio da eBay, mas sim ao tripod.com, que é um serviço de hospedagem grátis da Web. Essa era uma revelação involuntária de que o correio eletrônico não era legítimo. Mesmo assim, aposto que muitas pessoas inseriram suas informações nessa página, incluindo um número de cartão de crédito.

Esteja atento

Como usuários individuais da Internet, todos precisamos estar atentos, tomando decisões conscientes ao decidir se devemos inserir informações pessoais, senhas, números de conta, números de identificação e outras informações.

Quantas pessoas você conhece que poderiam lhe dizer se uma determinada página da Internet que estão vendo atende aos requisitos de uma página segura? Quantos empregados da sua empresa sabem o que devem procurar? *Todos* que usam a Internet devem saber o que é o pequeno símbolo que quase sempre aparece em algum lugar de uma página na Web com a forma de um cadeado. Eles devem saber que quando o cadeado está fechado, o site foi certificado como sendo seguro. Quando o cadeado está aberto ou o seu ícone não existe, o site Web não é autenticado como genuíno, e todas as informações transmitidas não estão criptografadas.

Entretanto, um atacante que consegue comprometer os privilégios administrativos de um computador da empresa pode modificar ou corrigir o código do sistema operacional para alterar a percepção do usuário daquilo que está realmente acontecendo. Por exemplo, as instruções de programação no software do browser que indicam que o certificado digital de um site Web é inválido podem ser modificadas para desviar da verificação. Ou então, o sistema pode ser modificado com algo chamado root kit, instalando uma ou mais *backdoors* no nível do sistema operacional, que são mais difíceis de serem detectadas.

Uma conexão segura autentica o site como genuíno e criptografa as informações que estão sendo comunicadas, de modo que um atacante não pode utilizar nenhum dado que seja interceptado. Você pode confiar em qualquer site Web, mesmo naquele que usa uma conexão segura? Não, porque o proprietário do site pode não estar atento para a aplicação de todas as correções de segurança necessárias, nem pode

Jargão

BACKDOOR Um ponto de entrada oculto que fornece um caminho secreto para o computador de um usuário, o qual é desconhecido do usuário. Usado também pelos programadores que desenvolvem um programa de software para que possam entrar no programa para corrigir problemas.

estar forçando os usuários ou administradores a respeitarem as boas práticas de senhas. Assim sendo, você não pode assumir que nenhum site com suposta segurança não esteja vulnerável a um ataque.

O HTTP *{hypertext transfer protocol)* seguro ou o SSL *(secure sockets layer)* fornece um mecanismo automático que usa os certificados digitais não apenas para criptografar as informações que estão sendo enviadas para o site distante, mas também para fornecer a autenticação (uma garantia de que você está se comunicando com o site Web verdadeiro). Entretanto, esse mecanismo de proteção não funciona para os usuários que não prestam atenção se o nome do site que é exibido na barra de endereços é, na verdade, o endereço correto do site que estão tentando acessar

Outra questão de segurança, a qual é amplamente ignorada, aparece como uma mensagem de aviso que diz algo do tipo "Este site não é seguro ou o certificado de segurança expirou. Você quer entrar no site mesmo assim?". Muitos usuários da Internet não entendem a mensagem e, quando ela aparece, simplesmente clicam em OK ou Sim e continuam com o seu trabalho, sem saber que podem estar em areia movediça. Cuidado: em um site Web que não usa um protocolo seguro, você nunca deve inserir nenhuma informação confidencial, tal como o seu endereço ou o número de telefone, os números do cartão de crédito ou do banco, ou qualquer outra coisa que deseja que continue sendo confidencial.

Thomas Jefferson disse que o preço da liberdade é a "eterna vigilância". A manutenção da privacidade e da segurança em uma sociedade que usa as informações como moeda também exige isso.

Tomando-se especialista em vírus

Uma nota especial sobre o software de vírus: é essencial para a intranet corporativa, mas também é essencial para cada empregado que usa um computador. Além de terem o software antivírus instalado em suas máquinas, os usuários obviamente precisam ter o netshield ativo (o que muitas pessoas não gostam porque ele inevitavelmente deixa mais lentas algumas funções do computador).

Com o software antivírus há outros procedimentos importantes que devem ser lembrados: as definições de vírus devem estar sempre atualizadas. A menos que a sua empresa esteja preparada para distribuir o software ou as atualizações pela rede para cada usuário, cada funcionário deve assumir a responsabilidade de fazer o download do conjunto mais recente de definições de vírus por conta própria. A minha recomendação é que todos configurem as opções do software de antivírus para que as novas definições de vírus sejam atualizadas automaticamente todos os dias.

Jargão

SECURE SOCKETS LAYER Um protocolo desenvolvido pela Netscape que fornece a autenticação para o cliente e o servidor em uma comunicação segura na Internet.

Em termos simples, você está vulnerável, a menos que as definições de vírus sejam regularmente atualizadas. E mesmo assim, você ainda não está completamente seguro contra os vírus ou worms que as empresas de software antivírus ainda não conhecem ou para os quais elas ainda não publicaram uma "vacina" padrão de detecção.

Todos os empregados que têm privilégios de acesso remoto de seus laptops ou dos computadores domésticos precisam no mínimo atualizar o software de vírus e um firewall pessoal em suas máquinas. Um atacante sofisticado olha o quadro geral para buscar o elo mais fraco e é nesse ponto que ele ataca. Uma responsabilidade corporativa é lembrar regularmente as pessoas que têm computadores remotos da necessidades de atualizar os firewalls pessoais e manter o software de vírus ativo, porque você não pode esperar que os funcionários, gerentes, vendedores e outros usuários remotos de um departamento de TI lembrem-se sozinhos dos perigos de deixar seus computadores desprotegidos.

Além dessas providências, recomendo o uso dos pacotes menos comuns, mas não menos importantes, que protegem contra os ataques dos Cavalos de Tróia, os chamados softwares antíTrojans. Quando este livro foi escrito, dois dos melhores programas eram o The Cleaner (www.moosoft.com) e o Trojan Defence Suite (www.diamondes.com.au).

Finalmente, talvez a mais importante mensagem de segurança para as empresas que não examinam as mensagens de correio eletrônico perigosas no gateway corporativo seja que tendemos a nos esquecer ou negligenciar as coisas que parecem periféricas para fazer o nosso trabalho, e os empregados precisam ser sempre lembrados de várias maneiras para não abrir os anexos de correio eletrônico, a menos que tenham certeza de que a fonte é uma pessoa ou organização em quem eles podem confiar. E a administração também precisa lembrar os empregados de que devem usar software de vírus ativo e software antiTrojan, que fornece uma proteção valiosa contra a mensagem de correio eletrônico aparentemente confiável, mas que pode conter uma carga destrutiva.

Capítulo 8

Usando a Simpatia, a Culpa e a Intimidação

Como discutido no Capítulo 15, um engenheiro social usa a psicologia da influência para levar o seu alvo a atender a sua solicitação. Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções tais como medo, agitação ou culpa. Eles fazem isso usando os gatilhos psicológicos — os mecanismos automáticos que levam as pessoas a responderem às solicitações sem uma análise cuidadosa das informações disponíveis.

Todos queremos evitar as situações difíceis para nós mesmos e para os outros. Com base nesse impulso positivo, o atacante pode jogar com a simpatia de uma pessoa, fazer a sua vitima se sentir culpada ou usar a intimidação como uma arma.

Aqui estão algumas lições das táticas mais conhecidas que jogam com as emoções.

UMA VISITA AO ESTÚDIO

Você já observou como uma pessoa pode passar pela segurança na porta de uma festa, de alguma reunião particular ou mesmo entrar em um restaurante *e* passar pela segurança sem que peçam o seu convite ou reserva?

Mais ou menos da mesma forma, um engenheiro social pode entrar nos lugares que você acharia não ser possível — como mostra esta história sobre a indústria do cinema.

A ligação telefônica

"Escritório de Ron Hillyard, Dorothy."

"Dorothy, oi. Meu nome é Kyle Bellamy. Acabei de ser contratado para trabalhar no Desenvolvimento de Animação da equipe de Brian Glassman. Vocês, sem dúvida, fazem as coisas de modo diferente por aqui."

Acho que sim. Nunca trabalhei em nenhum outro estúdio e não sei com certeza. Como posso ajudá-lo?"

"Para dizer a verdade, estou me sentindo meio burro. Tenho um autor que vem esta tarde para uma sessão e não sei com quem devo falar para que ele seja atendido. O pessoal aqui do escritório do Brian é simpático, mas odeio incomodá-los perguntando como faço isto, como faço aquilo. Como se eu estivesse na escola primária e não soubesse onde era o banheiro. Você me entende, não?"

Dorothy riu.

"Se você quer falar com a Segurança disque 7 e, em seguida, 6138. Se a Lauren atender, diga a ela que Dorothy disse que tomaria conta de você."

"Obrigado, Dorothy. E se não puder encontrar o banheiro, ligo de novo para você!"

Eles riram da idéia e desligaram.

A história de David Harold

Adoro cinema e quando me mudei para Los Angeles, achei que encontraria todo tipo de pessoa ligada ao cinema e que eles me convidariam para festas, me levariam para almoçar nos estúdios. Bem, já estava lá há um ano, estava para fazer 26 anos e o mais próximo que cheguei foi um tour pela Universal Studios com todo aquele pessoal camarada de Fenix e Cleveland. Assim sendo, finalmente chegamos ao ponto que eu imaginava: se eles não me convidam, eu me convido. E foi isso que fiz.

Comprei um exemplar do *Los Angeles Times* e li a coluna de entretenimento durante alguns dias, escrevi os nomes de alguns procedimentos dos diferentes estúdios. Resolvi tentar atacar um dos grandes estúdios primeiro.

Liguei para a telefonista e pedi para falar com o escritório desse produtor sobre o qual eu lera no jornal. A secretária que atendeu parecia do tipo maternal e achei que tive sorte; se fosse alguma jovem que estava lá apenas esperando ser descoberta, ela provavelmente não me daria a menor atenção.

Mas essa Dorothy parecia alguém que levava para casa um gatinho perdido, alguém que sentia pena do rapaz que estava se sentindo um pouco deslocado no emprego novo. Sem dúvida, eu havia conseguido o modo certo de falar com ela. Não é todo dia que você engana alguém e essa pessoa lhe dá mais até do que você pediu. Com pena, ela não apenas me deu o nome de uma das pessoas da Segurança, como também disse que eu deveria dizer a ela que a Dorothy queria que ela me ajudasse.

Obviamente eu havia planejado usar o nome de Dorothy de qualquer maneira. Isso tornou tudo melhor. Lauren abriu as portas imediatamente e nunca se importou em procurar o nome que dei no banco de dados para saber se ele estava realmente no banco de dados de empregado.

Quando cheguei ao portão naquela tarde, eles não apenas tinham o meu nome na lista de visitantes, como até tinham um lugar no estacionamento para mim. Eu havia almoçado tarde e fiquei passeando até o final do dia. Até me infiltrei em alguns cenários e observei como eles faziam os filmes. Não saí antes das 19 horas. Esse foi um dos dias mais incríveis que já tive.

Analisando a trapaça

Todo mundo já foi empregado novo um dia. Todos temos lembranças de como foi aquele primeiro dia, particularmente quando somos jovens e inexperientes. Assim sendo, quando um empregado novo pede ajuda, ele pode esperar que muitas pessoas — principalmente o pessoal do nível iniciante — se lembre de seus próprios sentimentos de "garoto novo na escola" e lhe dêem ajuda. O engenheiro social sabe disso e entende que pode usar esse fato para jogar com a simpatia de suas vítimas.

Facilitamos bastante a vida dos estranhos que querem dar um golpe para entrar nas fábricas e nos escritórios da nossa empresa. Mesmo com guardas nas portas e procedimentos de registro para todos que não são empregados, qualquer uma das diversas variações do golpe usadas nesta história permite que um intruso obtenha um crachá de visitante e entre tranqüilamente. E se a sua empresa exigir que os visitantes sejam acompanhados? Essa é uma boa regra, mas ela só é efetiva quando os

seus empregados estão conscientes sobre como impedir que alguém sozinho com ou sem crachá entre e como questioná-lo. E, em seguida, se as respostas não forem satisfatórias, os seus empregados têm de estar dispostos a entrar em contato com a segurança.

Ao facilitar que estranhos entrem nas suas instalações, você põe em perigo as informações confidenciais da empresa. Na época atual, com a ameaça de ataques terroristas pairando sobre nossa sociedade, não são apenas as informações que estão em risco.

"FAÇA ISSO AGORA"

Nem todos que usam as táticas da engenharia social são engenheiros sociais bem educados. Todos que têm um conhecimento interno de determinada empresa podem se tornar perigosos. O risco é maior ainda para uma empresa que mantém em seus arquivos e bancos de dados as informações confidenciais sobre seus empregados, o que, obviamente, é feito pela maioria das empresas.

Quando os funcionários não são educados ou treinados para reconhecer os ataques da engenharia social, pessoas determinadas como a senhora da próxima história podem fazer coisas que os mais honestos acham ser impossível.

A história de Doug

As coisas não iam tão bem com Linda, e soube assim que conheci Erin que ela era a mulher da minha vida. Linda é um pouco... bem não é que ela seja instável, mas ela pode extrapolar um pouco quando fica aborrecida.

Disse-lhe com o máximo possível de delicadeza que ela teria de se mudar e a ajudei a fazer as malas e até mesmo deixei que levasse alguns CDs do Queensryche que eram meus. Assim que ela saiu, fui a uma loja de ferragens comprar um novo cadeado para colocar na porta da frente e o coloquei naquela mesma noite. Na manhã seguinte, liguei para a empresa de telefonia e pedi para mudar o número do meu telefone e não dei permissão para que ele fosse divulgado.

Isso me deixava livre para procurar Erin.

A história de Linda

De qualquer forma eu já estava pronta para ir embora. Só não havia resolvido quando. Mas ninguém gosta de se sentir rejeitado. Assim sendo, tudo era só uma questão de "o que eu poderia fazer para que ele soubesse que era um idiota?".

Não foi preciso muito tempo para descobrir. Tinha de ser outra garota, caso contrário ele não me faria sair correndo daquele jeito. Eu esperaria um pouco e começaria a ligar para ele tarde da noite. Você sabe, naquela hora em que a última coisa que eles iriam querer seria um telefone tocando.

Aguardei até o próximo final de semana e liguei lá pelas 23 horas do sábado. Só que ele havia mudado o número do telefone. E o número novo não estava na lista. Isso só mostra o canalha que ele era.

Isso não era um problema muito grande. Comecei a procurar nos papéis que consegui levar antes de sair do meu emprego na empresa de telefonia. E lá estava ele — eu havia guardado um pedido de conserto de uma vez que houve um problema com a linha de telefone na casa do Doug e a listagem relacionava o cabo e o par do seu telefone.

Você sabe, é possível mudar o número do telefone como quiser, mas ele continua tendo o mesmo par de fios de cobre indo da sua casa até a central da empresa de telefonia, a qual é chamada de Escritório Central ou EC. O conjunto de fios de cobre de toda casa e apartamento é identificado por esses números, os quais são chamados de cabo e par. E se você souber como a empresa de telefonia faz as coisas, o que eu sei, só é preciso ter o cabo e o par para descobrir o número do telefone.

Eu tinha uma lista que dava todos os EC da cidade, com seus endereços e números de telefone. Procurei o número do EC do bairro onde eu morava com Doug, o canalha, e liguei, mas naturalmente ninguém atendeu. Onde está o operador quando você realmente precisa dele? Em 20 segundos já tinha um plano. Comecei a ligar para os outros EC e finalmente o localizei. Mas ele estava a quilômetros de distância e talvez de pernas para o ar sem fazer nada. Sabia que ele não ia querer fazer aquilo que eu precisava. Eu estava pronta com o meu plano.

"Aqui é Linda. Centro de Consertos", disse. "Temos uma emergência. O serviço em uma unidade de paramédicos parou. Temos um técnico na área tentando restaurar o serviço, mas não podemos localizar o problema. Precisamos que você vá até o EC Webster imediatamente para ver se temos discagem por tom saindo do escritório central."

Em seguida, continuei: "Ligo quando você chegar lá", porque obviamente não poderia pedir para ele ligar para o Centro de Consertos para falar comigo. Eu sabia que ele não sairia do conforto do escritório central para enfrentar o gelo acumulado no seu pára-brisa e dirigir àquela hora da noite. Mas essa era uma "emergência" e ele não poderia dizer que estava ocupado demais.

Quando liguei para ele 45 minutos mais tarde, no EC Webster, expliquei para ele verificar o cabo 29 e o par 2481, e ele foi até o quadro, verificou e respondeu: "Sim havia discagem por tom." E claro que eu sabia disso.

Depois acrescentei; "Muito bem, preciso que faça uma VL", uma verificação de linha, ou seja, pedi que identificasse o número do telefone. Ele faz isso discando para um número especial que lê o número do qual ele ligou. Ele não sabia se esse era um número que não estava na lista ou que mudou. e fez o que pedi. Pude ouvir o número sendo anunciado no seu telefone de teste de técnico. Tudo funcionou perfeitamente.

Repliquei: "Bem o problema deve estar na área", como se eu soubesse o número. Agradeci, disse que continuaríamos trabalhando para descobrir o problema e dei boa noite.

Recado do Mitnick

Quando um engenheiro social sabe como as coisas funcionam dentro da empresa-alvo, ele pode usar esse conhecimento para desenvolver a confiança junto aos empregados. As empresas precisam estar preparadas para os ataques da engenharia social vindos de empregados atuais ou ex-empregados, que podem ter um motivo de descontentamento. As verificações de histórico podem ser úteis para detectar os candidatos a emprego que tenham uma propensão para esse tipo de comportamento. Mas, na maioria dos casos, é difícil detectar essas pessoas. A única segurança razoável nesses casos é implantar e auditar os procedimentos de verificação de identidade, incluindo o status de emprego da pessoa, antes de divulgar qualquer informação para qualquer um que não se conheça pessoalmente e, portanto, não se sabe se ainda está na empresa.

Agora chega da história do Doug e da sua tentativa de se esconder de mim por trás de um número de telefone que não estava na lista. A diversão só estava começando.

Analisando a trapaça

A jovem da história pôde obter as informações que desejava para executar a sua vingança porque tinha o conhecimento interno: os números de telefone, os procedimentos e a linguagem da empresa de telefonia. Com isso ela não apenas pôde descobrir um novo número que não estava na lista, mas também pôde fazê-lo no meio de uma noite gelada, enviando um técnico de telefones para procurar um número pela cidade para ela.

"O SR. BIGG QUER ISSO"

Uma forma popular e eficaz de intimidação — popular em larga escala porque é muito simples — influencia o comportamento humano usando a autoridade.

Só o nome do assistente do escritório do CEO já pode ser valioso. Os detetives particulares e até mesmo os *head hunters* fazem isso o tempo todo. Eles ligam para a telefonista e dizem que querem falar com o escritório do CEO. Quando a secretária ou o assistente executivo respondem, dizem que têm um documento ou um pacote para o CEO ou, se enviarem um anexo de e-mail, perguntam se eles poderiam imprimi-lo ou então perguntam qual é o número do fax. E, por falar nisso, qual é o seu nome?

Em seguida, ligam para a próxima pessoa e dizem: "Jeannie do escritório do Sr. Bigg me disse para ligar para você e pedir ajuda com alguma coisa." Essa técnica chama-se advocacia administrativa e geralmente é usada como um método de estabelecer rapidamente a confiança, influenciando o alvo para que ele acredite que o atacante tem relações com alguém que tem autoridade. Um alvo tem mais chances de prestar um favor para alguém que conhece alguém que ele conhece.

Se o atacante tiver acesso a informações confidenciais, ele pode usar esse tipo de abordagem para gerar e manipular emoções úteis na vítima, tais como o medo de causar problemas para os seus superiores. Este é um exemplo típico.

A história de Scott

"Scott Abrams."

"Scott, aqui é Christopher Dalbridge. Acabei de falar ao telefone com o Sr. Biggley e ele estava muito descontente. Disse que pediu há dez dias para vocês nos enviarem cópias de toda a sua pesquisa de penetração de mercado para análise. E nunca recebemos nada."

"Pesquisa de penetração de mercado? Ninguém me disse nada sobre isso."

"Em qual departamento você trabalha?"

"Somos uma empresa de consultoria contratada e já estamos atrasados."

"Ouça, estou indo para uma reunião agora. Me deixe o seu número de telefone e...".

O atacante agora parecia estar frustrado: "E isso o que você quer que eu diga ao Sr. Biggley?! Ouça, ele espera a nossa análise amanhã de manhã e temos de trabalhar hoje à noite. Agora, você quer que *eu* diga a ele que não conseguimos porque não recebemos o relatório de vocês ou quer dizer isso a ele pessoalmente?"

Um CEO zangado pode arruinar a sua semana. O alvo provavelmente vai resolver que talvez seja melhor ele cuidar disso antes de ir para aquela reunião. Novamente, o engenheiro social apertou o botão certo para receber a resposta que desejava.

Analisando a trapaça

O truque da intimidação mencionando uma autoridade funciona bem se a outra pessoa ocupar um nível relativamente baixo dentro da empresa. O uso do nome de uma pessoa importante não apenas supera a relutância normal ou a suspeita, mas também torna a pessoa mais disposta a agradar; o instinto natural de querer ser útil se multiplica quando você acha que a pessoa que está ajudando é importante ou influente,

O engenheiro social sabe, porém, que, ao executar este truque, é melhor usar o nome de alguém que tem um nível mais alto do que o chefe da própria pessoa. E este truque é complicado dentro de uma organização pequena: o atacante não quer que a sua vítima por acaso faça este comentário com o vice-presidente de marketing: "Enviei o plano de marketing de produto para aquele consultor que você pediu para me ligar." Isso pode produzir a resposta: "Que plano de marketing? Que consultor?" E isso pode levar à descoberta de que a empresa foi vítima de um truque.

Recado do Mitnick

A intimidação pode criar o medo de ser punido e influenciar as pessoas para que cooperem. Pode também criar o medo de uma situação embaraçosa ou de ser desqualificado para a nova promoção.

As pessoas devem ser treinadas para saber que não apenas é aceitável, mas também esperado o desafio à autoridade quando a segurança está em jogo. O treinamento para a segurança das informações deve incluir o ensino de como desafiar a autoridade de maneiras amistosas ao cliente, sem danificar os relacionamentos. Além disso, essa expectativa deve receber suporte de cima para baixo. Se um empregado não tiver apoio ao desafiar as pessoas independentemente de seus status, a reação normal é parar o desafio — exatamente o oposto daquilo que você quer.

O QUE A ADMINISTRAÇÃO DO SEGURO SOCIAL SABE SOBRE VOCÊ ?

Gostamos de achar que os órgãos do governo que têm informações sobre nós mantêm essas informações muito bem trancadas, longe das pessoas que não têm uma necessidade verdadeira de conhecê-las. A verdade é que até mesmo o governo federal não está imune às invasões, como gostaríamos de pensar.

A ligação telefônica de May Linn

Local: Um escritório regional da Administração do Seguro Social

Hora: 10hl8, manhã de terça-feira

"Módulo três. Aqui é May Linn Wang."

A voz do outro lado do telefone parecia estar pedindo desculpas e era quase tímida.

"Srta. Wang, aqui é Arthur Arondale do Escritório do Inspetor Geral. Posso chamá-la de 'May'?"

"Aqui é 'May Linn"', ela repetiu.

"Bem, May Linn, temos um funcionário novo aqui que ainda não tem um computador, e agora mesmo ele tem um projeto de prioridade e está usando o meu. Somos do governo dos Estados Unidos e eles dizem que não têm dinheiro no orçamento para comprar um computador para ele usar. E agora o meu chefe acha que eu estou me atrasando e não quer ouvir nenhuma desculpa, sabe como é?"

"Entendo bem o que você quer dizer."

"Você pode ajudar com uma consulta rápida ao MCS?", ele perguntou, usando o nome do sistema de computadores onde estão armazenadas as informações sobre os contribuintes.

"Certamente, do que você precisa?"

"A primeira coisa que preciso fazer é uma alfadent de Joseph Johnson, data de nascimento 4/7/69". (Alfadent significa pesquisa por ordem alfabética no computador pelo nome do contribuinte, o qual também é identificado pela data de nascimento.)

Após uma breve pausa, ela perguntou:

"O que você precisa saber?"

"Qual é o seu número de conta?", ele explicou, usando o atalho interno para o número do seguro social. Ela leu o número.

"Muito bem, preciso que você faça um numident daquele número de conta", acrescentou o interlocutor.

Essa era uma solicitação para que ela lesse os dados básicos do contribuinte, e May Linn respondeu dando o local de nascimento do contribuinte, o nome de solteira da mãe e o nome do pai. O interlocutor ouviu pacientemente enquanto ela também lhe dava o mês e ano em que o cartão fora emitido e o distrito no qual fora emitido.

A seguir ele pediu um DEQY, que é a abreviatura de "consulta detalhada de rendimentos".

Após a solicitação do DEQY, ele teve a resposta "Para qual ano?". O interlocutor respondeu "Para o ano 2001".

May Linn continuou: "O valor foi de US$ 190.286 e o pagador foi a Johnson MicroTech."

"Alguma outra remuneração?"

"Não."

"Obrigado", ele disse. "Você foi muito gentil."

Em seguida, ele tentou tomar providências para ligar para ela sempre que precisasse de informações e não tivesse acesso ao seu computador, usando novamente o truque favorito dos engenheiros sociais de sempre tentar estabelecer uma conexão para poder voltar à mesma pessoa e evitar o aborrecimento de ter de encontrar uma nova vítima todas as vezes.

"Não na próxima semana", ela salientou, porque ia para Kentucky para o casamento da irmã. Qualquer outra época ela faria o que fosse possível.

Ao desligar o telefone, May Linn sentiu-se bem por ter podido ajudar um pouco um colega servidor público a quem não davam o devido valor.

A história de Keith Carter

A julgar pelos filmes e romances policias mais vendidos, um detetive particular tem pouca ética e muito conhecimento de como obter as melhores informações sobre as pessoas. Eles fazem isso usando métodos ilegais, enquanto mal conseguem evitar a prisão. Obviamente, a verdade é que a maioria dos detetives particulares tem empresas legítimas. Como muitos deles começaram a vida profissional como oficiais de justiça, sabem perfeitamente bem o que é e o que não é legal, e a maioria não se sente tentada a cruzar a linha da ilegalidade.

Entretanto, existem exceções. Alguns detetives particulares — mais do que alguns, na verdade — parecem-se com os personagens das histórias policiais. Eles são conhecidos no meio como informantes, um termo educado para as pessoas que estão dispostas a quebrar as regras. Eles sabem que podem realizar qualquer tarefa muito mais rapidamente e de modo bem mais fácil se tomarem alguns atalhos. O fato de esses atalhos serem crimes em potencial, que podem colocá-los atrás das grades por alguns anos, não parece deter aqueles mais inescrupulosos.

Nesse meio tempo, os detetives particulares do primeiro escalão — aqueles que trabalham em um escritório bonito em uma parte valorizada da cidade — não fazem esse tipo de trabalho. Eles apenas contratam algum informante para fazer isso para eles.

O rapaz que chamaremos de Keith Carter era o tipo de "olheiro" particular sem ética.

Ele era um caso típico de "Onde ele está escondendo o dinheiro?". Ou também "Onde ela está escondendo o dinheiro?". Eventualmente podia ser uma senhora rica que queria saber onde o seu marido havia escondido o seu dinheiro (embora o motivo pelo qual uma mulher rica se casa com um homem sem dinheiro era um enigma no qual Keith Carter sempre pensava sem nunca encontrar uma boa resposta).

Neste caso, o marido cujo nome era Joe Johnson, era quem estava congelando o dinheiro. Ele era um homem muito inteligente que havia fundado uma empresa de alta tecnologia com US$ 10 mil que emprestara da família da sua mulher, e havia aumentado o patrimônio da empresa para US$ 100 milhões. De acordo com o advogado do seu divórcio, ele havia escondido seus bens, e o advogado queria um relatório completo.

Keith calculou que o seu ponto de partida seria a Administração do Seguro Social, particularmente os arquivos sobre Johnson, os quais estariam cheios de informações muito úteis para uma situação como essa. Munido dessas informações, Keith poderia fingir ser o alvo e ir aos bancos, corretoras e instituições fora do país para contar-lhes tudo.

A sua primeira ligação foi para o escritório de um distrito local, usando o mesmo número 0800 que qualquer pessoa usa e que está relacionado na lista telefônica. Quando o atendente respondeu, Keith pediu para ser transferido para alguém da seção de Reclamações. Outra espera e, em seguida, uma voz atendeu. Agora Keith mudou de lado: "Oi", ele começou. "Aqui é Gregory Adams, do Escritório Distrital 329. Ouça, estou tentando acessar um fiscal de reclamações que trata de um número de conta que termina com 6363 e o número que tenho é de um aparelho de fax".

"Aqui é o Módulo 2", disse o homem que atendeu. Ele procurou o número e o forneceu para Keith.

A seguir, ele ligou para o Módulo 2. Quando May Linn respondeu, ele trocou de chapéu e continuou com a rotina de ser do Escritório do Inspetor Geral e estar com problemas em usar o seu com-

putador. porque outra pessoa o eslava usando. Ela deu-lhe as informações que ele queria e concordou em fazer o que fosse possível quando ele precisasse de ajuda no futuro.

Analisando a trapaça

O que torna essa abordagem eficaz é o truque de atrair a simpatia do empregado com a história de outra pessoa que está usando o computador e que o "meu chefe não está feliz comigo". As pessoas não mostram suas emoções no trabalho com freqüência. Quando fazem isso, a tendência é derrubar as defesas normais de outra pessoa contra os ataques da engenharia social. O truque emocional de "Eu estou com problemas, você pode me ajudar?" foi tudo do que ele precisou para ganhar o dia.

Insegurança Social

Por incrível que pareça, a Administração do Seguro Social postou uma cópia de lodo o seu Manual de Operações do Programa na Web, cheio de informações úteis para o seu pessoal. mas que também são valiosíssimas para os engenheiros sociais. Ele contém abreviações, jargão e instruções sobre como solicitar aquilo que você quer, como descreveu essa história.

Você quer aprender mais sobre as informações internas da Administração do Seguro Social? Basta pesquisar no Google ou digitar este endereço no seu browser: http://policy.ssa.gov/poms.nsf/. A menos que a agência já tenha lido esta história e tenha removido o manual, quando estiver lendo este livro, você encontrará instruções on-line que fornecem informações detalhadas sobre quais dados um funcionário da ASS pode dar para a comunidade. Em termos práticos, essa comunidade inclui todo engenheiro social que possa convencer um funcionário da ASS que ele também é um funcionário.

O atacante não obteria essas informações de um funcionário que atende o público em geral pelo telefone. O tipo de ataque usado por Keith só funciona quando a pessoa que recebe a ligação é alguém cujos números de telefone não estão disponíveis para o público e que, portanto, tem a expectativa de que uma pessoa que ligue deve ser alguém de dentro — outro exemplo da segurança speakeasy.

Os elementos que ajudaram nesse ataque incluem:

- Saber o número do telefone do Módulo.
- Saber a terminologia que eles usam — numident, alfadent e DEQY.
- Fingir ser do escritório do Inspetor Geral, o qual todo funcionário do governo federal sabe que é uma agência de investigações do governo com poderes amplos. Isso dá ao atacante uma aura de autoridade.

Um ponto interessante: os engenheiros sociais parecem saber como fazer as solicitações para que quase ninguém pense "Por que você está ligando para *mim?"* — mesmo quando logicamente faria mais sentido se a ligação tivesse sido encaminhada para outra pessoa em algum departamento diferente. Talvez ajudar alguém apenas represente uma quebra na monotonia diária e a vítima dá um desconto para o fato de a ligação parecer incomum.

Finalmente, o atacante desse incidente, não satisfeito em obter as informações apenas para o caso do momento, queria estabelecer um contato que pudesse usar regularmente. Ele também poderia ter

usado um truque comum no ataque pela simpatia — "Derrubei café no meu teclado". Isso não serviria aqui. porém, porque um teclado pode ser trocado em um dia. Por esse motivo, ele usou a história de outra pessoa que estava usando o seu computador, o que poderia durar semanas. "Sim, achei que ele teria o seu próprio computador ontem, mas veio um e outro funcionário fez algum tipo de acordo e conseguiu ficar com ele. Assim sendo, esse chato ainda está aqui na minha sala". E assim por diante.

Coitadinho de mim, preciso de ajuda. E preciso fazer um pouco de charme.

UMA LIGAÇÃO SIMPLES

Uma das principais preocupações de um atacante é fazer a sua solicitação parecer *razoável* — algo típico das solicitações que surgem no dia de trabalho da vítima, algo que não distrai muito a atenção da vítima. Assim como acontece com muitas outras coisas na vida. fazer com que uma solicitação pareça lógica pode ser um desafio hoje, mas amanhã isso pode ser muito fácil.

A ligação de Mary H.

Data/Hora: segunda-feira, 23 de novembro, 7h49.

Local: Mauersby & Storch Accounting, Nova York

Para a maioria das pessoas, o trabalho de contabilidade resume-se a somar números e contar feijões e é visto como sendo tão agradável quanto fazer um tratamento de canal. Felizmente, nem todos vêem o trabalho dessa forma. Mary Harris, por exemplo, achava que o seu trabalho como contadora-chefe era muito interessante, e por isso ela era uma das funcionárias mais dedicadas da contabilidade da sua empresa.

Nessa segunda-feira em particular, Mary chegou cedo para começar logo aquilo que esperava ser um longo dia, e ficou surpresa quando o seu telefone tocou. Ela atendeu e deu seu nome.

"Oi, aqui é Peter Sheppard. Sou da Arbuckle Support, a empresa que faz o suporte técnico para vocês. Registramos algumas reclamações no final de semana de pessoas que tiveram problemas com os computadores daí. Pensei em resolver isso antes que todos chegassem esta manhã para trabalhar. Você está tendo algum problema com o seu computador ou com a sua conexão de rede?"

Ela disse que ainda não. Ligou o computador e, durante a inicialização, ele explicou o que queria fazer.

"Gostaria de realizar alguns testes com você", ele disse. "Posso ver na minha tela as teclas que você digita e quero ter certeza de que estão passando pela rede corretamente. Assim sendo, cada vez que você digitar uma tecla, quero que me diga qual é a tecla para eu ver se a mesma letra ou número estão aparecendo aqui. OK?"

Com visões do pesadelo que seria se o seu computador não funcionasse e do dia frustrante que seria não poder trabalhar, ela ficou mais do que feliz em ter esse homem para ajudá-la. Após alguns instantes, ela retrucou: "Tenho a tela de login e vou digitar o meu ID. Estou digitando agora — M... A... R... Y... D."

"Até aqui tudo bem", ele afirmou. "Estou vendo isso aqui. Agora digite a sua senha, mas não me diga qual é. Você nunca deve dizer a ninguém qual é a sua senha, nem mesmo ao suporte técnico. Vou ver os asteriscos aqui — **a** sua senha está protegida e não posso vê-la." Nada disso era verdade, mas fazia sentido para Mary. Em seguida, ele continuou: "Me avise quando o seu computador inicializar."

Quando ela disse que o computador estava funcionando, ele pediu para ela abrir dois aplicativos e ela disse que eles haviam iniciado "bem".

Mary estava aliviada ao ver que tudo parecia estar funcionando normalmente. Peter disse: "Fico contente de saber que você poderá usar o seu computador", e continuou: "nós acabamos de instalar uma atualização que permite que as pessoas mudem suas senhas. Você poderia perder mais alguns minutos para eu ver se está tudo funcionando direito?"

Ela estava agradecida pela ajuda que ele havia dado e concordou prontamente. Peter narrou as etapas para abrir o aplicativo que permite que um usuário mude as senhas, um elemento-padrão do sistema operacional Windows 2000. "Agora insira a sua senha", ele pediu. "Mas lembre-se de não dizê-la em voz alta."

Quando ela terminou, Peter acrescentou: "Só para este teste, quando o sistema pedir a nova senha digite 'test123'. Em seguida, digite novamente na caixa Verificação e clique em Enter."

Ele disse como ela deveria se desconectar do servidor. Pediu para ela aguardar alguns minutos antes de se conectar novamente, desta vez tentando fazer o logon com a nova senha. Tudo funcionou muito bem, Peter parecia muito satisfeito e fez com que ela mudasse de volta para a senha original ou selecionasse uma nova — e mais uma vez avisou para ela não falar a senha em voz alta.

"Bem, Mary", Peter finalizou. "Não encontramos nenhum problema e isso é ótimo. Ouça, se surgir algum problema, ligue para nós aqui na Arbuckle. Geralmente trabalho em projetos especiais, mas qualquer pessoa que atender pode ajudá-la." Ela agradeceu e eles se despediram.

A história de Peter

A notícia corria sobre Peter — algumas das pessoas da sua comunidade que haviam estudado com ele ouviram falar que ele se transformara em um tipo de mago de computador que podia encontrar informações úteis que as outras pessoas não podiam obter. Quando Alice Conrad pediu-lhe um favor, a princípio ele se negou. Por que ajudaria? Certa vez, quando ele a convidou para sair, ela recusou.

Mas a sua recusa em ajudar não pareceu surpreendê-la. Ela disse que achava que ele não conseguiria fazer aquilo de qualquer maneira. Isso foi como um desafio, porque ele tinha certeza de que poderia. E foi assim que ele concordou em ajudá-la.

Alice havia recebido uma proposta para realizar um trabalho de consultoria para uma empresa de marketing, mas os termos do contrato não pareciam muito bons. Antes de voltar e pedir melhores condições, ela queria saber quais eram as condições que os outros consultores tinham em seus contratos.

Peter conta a história desta maneira:

Eu não disse a Alice, mas fujo de gente que quer que eu faça algo que elas acham que eu não posso fazer, quando sei que é fácil Bem, desta vez não era exatamente fácil. Isso me daria um pouco de trabalho. Mas tudo bem.

Eu podia mostrar para ela como eu era esperto.

Um pouco depois das 7h30 da manhã de segunda-feira liguei para os escritórios da empresa de marketing e falei com a recepcionista. Contei que era da empresa que cuidava dos planos de pensão e precisava falar com alguém da Contabilidade. Perguntei se ela sabia se alguém da Contabilidade já havia chegado. Ela disse: "Eu acho que vi Mary entrar há alguns minutos, vou tentar transferir."

Quando Mary atendeu o telefone, contei a minha história sobre os problemas no computador, a qual criei para fazer com que ela se sentisse feliz em cooperar. Assim que a ensinei a mudar a senha. rapidamente eu fiz o login no sistema com a mesma senha temporária que pedi para ela usar, testl23.

É aqui que entra a arte do plano — instalei um pequeno programa que me permitia acessar o sistema de computadores da empresa sempre que desejasse, usando uma senha secreta própria. Depois de falar com Mary. a minha primeira etapa foi apagar o controle de auditoria para que ninguém jamais soubesse que eu havia estado no sistema. Isso foi fácil. Após elevar meus privilégios de sistema, pude fazer o download de um programa grátis chamado *clearlogs* que encontrei em um site Web relacionado com segurança em www.ntsecurity.nu.

Agora estava na hora do trabalho de verdade. Fiz uma pesquisa de todos os documentos que tinham a palavra "contrato" no nome do arquivo e fiz o download dos arquivos. Em seguida, pesquisei um pouco mais e descobri o melhor — o diretório que continha todos os relatórios de pagamentos de consultoria. Assim sendo, juntei todos os arquivos de contratos e uma lista dos pagamentos.

Alice podia olhar os contratos e ver quanto eles estavam pagando para os outros consultores. Deixei que ela tivesse o trabalho de procurar em todos aqueles arquivos. Eu já havia feito o que ela me pedira.

Dos discos nos quais gravei os dados, imprimi alguns dos arquivos para mostrar as evidências para ela. Fiz com que ela me encontrasse para pagar o jantar. Você devia ter visto o seu rosto quando encontrou a pilhas de papéis. "Não acredito", ela afirmava. "Não acredito."

Não trouxe os discos comigo. Eles eram a isca. Disse que ela teria de ir pegá-los, esperando que ela talvez quisesse mostrar a sua gratidão pelo favor que havia prestado.

Recado do Mitnick

É incrível como é fácil para um engenheiro social convencer as pessoas a fazerem as coisas com base no modo como ele estrutura a solicitação. A tese é acionar uma resposta automática com base nos princípios psicológicos e utilizar os atalhos mentais que as pessoas usam quando percebem que o interlocutor é um aliado.

Analisando a trapaça

A ligação telefônica de Peter para a empresa de marketing representava a forma mais básica de engenharia social — uma única tentativa que precisou de pouca preparação, funcionou na primeira vez e levou apenas alguns minutos.

Melhor ainda era o fato de que Mary (a vítima) não tinha motivo para achar que havia caído em algum tipo de truque, nenhum motivo para fazer um relatório ou fazer alarde.

O esquema funcionou porque Peter usou três táticas da engenharia social. Em primeiro lugar, ele conseguiu a cooperação inicial de Mary, gerando o medo — fazendo com que ela pensasse que o computador não poderia ser usado. Em seguida, ele se deu ao trabalho de fazer com que ela abrisse dois dos seus aplicativos para que tivesse certeza de que eles estavam funcionando bem, fortalecendo assim a confiança entre os dois, ou a idéia de serem aliados. Finalmente, ele conseguiu mais cooperação para a parte essencial dessa tarefa jogando com a sua gratidão pela ajuda que ele havia fornecido, garantindo que o seu computador estava funcionando bem.

Dizendo a ela que nunca revelasse a sua senha, nem mesmo para ele, Peter fez um trabalho completo e sutil, convencendo-a de que ele estava preocupado com a segurança dos arquivos da sua empresa. Isso aumentou a sua confiança no fato de que ele era verdadeiro, porque estava protegendo ela e a empresa.

A BATIDA DA POLÍCIA

Imagine esta cena: o governo estava tentando armar uma cilada para um homem chamado Arturo Sanchez, que vinha distribuindo filmes de graça pela Internet. Os estúdios de Hollywood diziam que ele violava seus direitos autorais, ele dizia que estava apenas tentando fazê-los reconhecer um mercado inevitável para começarem a disponibilizar filmes novos para download. Ele destaca (corretamente) que essa seria uma fonte enorme de renda para os estúdios, a qual parecem estar ignorando.

O mandado de busca, por favor

Certa noite ele chega tarde em casa e vê do outro lado da rua que as luzes do seu apartamento estão desligadas, embora sempre deixe uma ligada ao sair.

Ele bate na porta de um vizinho até que o homem acorda e descobre que houve mesmo uma batida policial no prédio. Mas eles fizeram os vizinhos permanecerem nas escadas e ele ainda não tem certeza do apartamento no qual eles estiveram. Ele só sabe que eles saíram levando coisas pesadas, mas elas estavam embrulhadas e ele não sabia o que eram. E não levaram ninguém algemado.

Arturo verifica o seu apartamento. A má notícia é que há um papel da polícia exigindo que ele ligue imediatamente e marque uma entrevista dentro de três dias. Pior ainda é o fato de que não encontrou seus computadores.

Arturo some na noite e vai para a casa de um amigo. Mas a incerteza o incomoda. Quanto a polícia sabe? Eles poderiam tê-lo pego finalmente, mas teriam dado a ele a chance de ele fugir? Ou é alguma outra coisa diferente, algo que ele pode esclarecer sem sair da cidade?

Antes de continuar lendo, pare e pense um pouco: você pode imaginar alguma maneira de descobrir o que a polícia quer saber sobre você? Supondo que você não tem nenhum contato político ou amigos no departamento de polícia ou no gabinete do promotor, será que há alguma maneira pela qual você, um cidadão comum, poderia obter essas informações? Ou que alguém com habilidades de engenheiro social poderia?

Enganando a polícia

Arturo atendeu a sua necessidade de saber desta maneira: para começar, conseguiu o número de telefone de uma copiadora próxima, ligou para eles e pediu seu número de fax.

Em seguida, ligou para o escritório do promotor distrital e pediu para falar com Registros. Quando foi transferido para o escritório de Registros, ele se apresentou como um investigador de Lake County e disse que precisava falar com o funcionário que arquiva as ações de busca ativas.

"Sou eu", respondeu a senhora. "Ah, ótimo", ele continuou. "Porque demos uma batida na casa de um suspeito ontem à noite e estou tentando localizar a declaração." "Elas são arquivadas por endereço", ela explicou.

Ele deu seu endereço e ela pareceu muito interessada. "Ah, sim", ela disse "Conheço *esse*. 'O golpe do copyright'."

Observação

Como um engenheiro social conhece os detalhes de tantas operações — departamentos de polícia, escritórios de promotoria, práticas da empresa de telefonia, a organização de empresas específicas que estão em áreas úteis para seus ataques, tais como telecomunicações e computadores? Porque descobrir é o seu negócio. Esse conhecimento é o bem de um engenheiro social porque as informações podem ajudá-lo em seus esforços para enganar.

"Esse mesmo", ele concordou. "Estou procurando a declaração e uma cópia do mandado."

"Certo, eles estão bem aqui."

"Ótimo", ele disse. "Ouça, estou fora e tenho uma reunião com o Serviço Secreto sobre esse caso em 15 minutos. Tenho estado tão distraído ultimamente, deixei o arquivo em casa e nunca vou chegar lá e voltar a tempo. Posso usar as suas cópias?"

"É claro, sem problemas. Vou fazer as cópias, você pode vir pegá-las."

"Isso é muito bom. Mas ouça, estou no outro lado da cidade. Você poderia me enviar as cópias por fax?"

Isso criava um pequeno problema, mas ele podia ser contornado. "Não lemos um fax aqui em Registros", ela retrucou. "Mas eles têm um na Secretaria e talvez me deixem usá-lo."

Ele disse: "Eu vou ligar para lá e verificar isso."

A senhora da Secretaria disse que poderia cuidar disso, mas queria saber "Quem iria pagar". Ela precisava de um código contábil.

"Vou conseguir o código e ligo de volta", ele disse a ela.

Em seguida, ele ligou para o escritório do promotor novamente, identificou-se como um policial e simplesmente perguntou à recepcionista: "Qual e o código contábil do escritório do promotor?" Ela respondeu sem hesitar.

A ligação de volta para o escritório da Secretaria para fornecer o número contábil deu-lhe a desculpa para se aproveitar um pouco mais da situação: ele convenceu a senhora a subir as escadas e pegar as cópias dos documentos a serem enviados por fax.

Cobrindo os rastros

Arturo ainda tinha umas etapas a serem cumpridas. Sempre havia a possibilidade de que alguém achasse algo estranho, e ele poderia chegar na copiadora e encontrar alguns detetives á paisana e tentando parecer ocupados até que alguém aparecesse pedindo um determinado fax. Ele aguardou um pouco e, em seguida, ligou novamente para o escritório da Secretaria para verificar se a senhora havia enviado o fax. Até aqui tudo bem.

Ele ligou para outra copiadora da mesma cadeia cio outro lado da cidade e disse como ele estava "satisfeito com o modo como eles realizavam o trabalho e queria escrever uma carta cumprimentando o gerente, qual era o seu nome?". Com essa informação essencial, ligou para a primeira loja da copiadora novamente e pediu para falar com o gerente. Quando o homem atendeu, Arturo explicou: "Oi, aqui é Edward da loja 628 em Hartfield. A minha gerente Anna pediu para eu ligar para você.

Temos um cliente que está aborrecido — alguém lhe deu o número do fax da loja errada. Ele está aqui aguardando um fax importante, só que o número que ele tem é da sua loja." O gerente prometeu pedir para localizarem o fax e o enviou para a loja de Hartfield imediatamente.

Arturo já estava esperando na segunda loja quando o fax chegou lá. Após pegá-lo, ligou novamente para o escritório da Secretaria para agradecer à senhora e disse: "Não é preciso levar essas cópias para cima, você pode simplesmente jogá-las fora agora". Em seguida, ligou para o gerente da primeira loja e disse para ele também jogar fora a sua cópia do fax. Dessa forma, não haveria nenhum registro do que ocorreu, apenas para o caso de alguém mais tarde vier fazer perguntas. Os engenheiros sociais sabem que cuidado nunca é demais.

Dessa forma, Arturo não leve nem de pagar taxas na primeira copiadora pelo recebimento do fax nem o seu envio para a segunda loja. E se a polícia aparecesse na primeira loja, Arturo já teria o seu fax e estaria longe quando conseguissem enviar alguém para a segunda localização.

O final da história: a declaração e o mandado mostravam que a polícia tinha evidencias bem documentadas das atividades de cópia de filmes de Arturo. Era isso o que ele precisava saber. À meia-noite já havia cruzado a fronteira do estado. Arturo estava a caminho de uma vida nova, em algum outro lugar, com uma nova identidade, pronto para recomeçar sua campanha.

Analisando a trapaça

As pessoas que trabalham nos escritórios de promotoria distritais estão sempre em contato com policiais — respondendo perguntas, tomando providências, anotando recados. Qualquer pessoa que tenha sangue frio suficiente para ligar e alegar ser um policial, representante do delegado ou outra coisa tem credibilidade. A menos que fique óbvio que a pessoa não conhece a terminologia, que ela está nervosa ou que não pareça autentica de alguma outra maneira, ela nem deverá apresentar provas de sua identidade. Foi exatamente isso que aconteceu aqui, com dois funcionários diferentes.

Recado do Mitnick

A verdade é que ninguém está imune contra ser enganado por um bom engenheiro social. Devido ao ritmo da vida normal, nem sempre pensamos com cuidado antes de tomarmos as decisões, mesmo em questões que são importantes para nós. As situações complicadas, a falta de tempo, o estado emocional ou a fadiga mental podem facilmente nos distrair. Assim sendo, tomamos um atalho mental e resolvemos sem analisar cuidadosamente as informações, um processo mental conhecido como resposta automática. Isso é válido até para os agentes da lei dos governos federal, estadual e municipal. Somos humanos.

A obtenção de um código de cobrança necessário foi resolvida com uma única ligação telefônica. Em seguida, Arturo usou o truque da simpatia com a história sobre "uma reunião com o Serviço Secreto em 15 minutos, tenho andado distraído e deixei o arquivo em casa". Naturalmente ela sentiu pena dele e fez o que podia para ajudar.

Em seguida, usando não uma, mas duas copiadoras, Arturo garantiu a segurança quando foi pegar o fax. Uma variação disso que torna mais difícil ainda rastrear o fax: em vez de mandar enviar o documento para outra copiadora, o atacante pode dar aquilo que parece ser um número de fax, mas que na verdade é um endereço de um serviço de Internet grátis que recebe um fax de graça e o enca-

minha automaticamente para o seu endereço de correio eletrônico. Dessa forma ele pode ser aberto diretamente no computador do atacante, e ele não precisa mostrar o rosto em um lugar onde mais tarde pode ser identificado. E o endereço de correio eletrônico e o número do fax eletrônico podem ser abandonados assim que a missão tenha sido completada.

VIRANDO A MESA

Um jovem que chamarei de Michael Parker era uma daquelas pessoas que descobrem um pouco tarde demais que os empregos com os melhores salários em sua maior parte vão para as pessoas com grau superior. Ele teve a chance de freqüentar uma faculdade local com bolsa parcial, além de empréstimos educacionais, mas isso significa trabalhar à noite e nos finais de semana para pagar o aluguel, a comida, a gasolina e o seguro do carro. Michael, que sempre gostava de encontrar atalhos, pensou que talvez houvesse outra maneira, uma que o recompensasse mais rapidamente e com menos esforço. Como vinha aprendendo sobre computadores desde a época em que começou a jogar, com a idade de dez anos, e se tornou fascinado em descobrir como eles funcionavam, ele resolveu saber se poderia "criar" sua própria formatura acelerada em ciência da computação.

Formando-se — sem louvor

Ele poderia ter invadido os sistemas de computadores da universidade estadual, encontrado o histórico de alguém que havia se formado com um B+ ou A médio, copiado o histórico, colocado seu próprio nome e incluído esse histórico nos registros da classe que se formava naquele ano. Pensando nisso, ele se sentia meio desconfortável com a idéia e percebeu que deveria haver outros históricos de um aluno que estivesse no *campus* — registros de pagamento de mensalidades, o escritório dos alojamentos e quem sabe mais o quê. A simples criação do histórico dos cursos e notas deixaria muitos buracos.

Pensando mais um pouco, ocorreu-lhe que poderia atingir seu objetivo vendo se a escola tinha um formando com mesmo nome que o seu, que havia se formado em ciência da computação em algum momento durante um período apropriado de anos. Se encontrasse esse aluno, ele poderia colocar o número do seguro social do outro Michael Parker nos formulários pedindo emprego; qualquer empresa que verificasse o nome e o número do seguro social junto à universidade saberia que, sim, ele tinha o diploma que dizia ter. (Não era muito óbvio para a maioria das pessoas, mas era óbvio para ele que poderia colocar um número de seguro social no formulário de emprego e, em seguida, se fosse contratado, colocaria o seu próprio número nos formulários de empregado novo. A maioria das empresas nem pensa em verificar se um novo contratado usou um número diferente no início do processo de contratação).

Conectando-se com problemas

Como encontrar um Michael Parker nos registros da universidade? Ele abordou esse problema desta maneira:

Ele foi à biblioteca principal do *campus* da universidade, sentou-se em um terminal de computador, entrou na Internet e acessou o site Web da universidade. Em seguida, ligou para a secretaria. Com a pessoa que atendeu, usou uma das rotinas agora conhecidas da engenharia social: "Estou falando do Centro de Computadores, estamos fazendo algumas mudanças na configuração da rede e queremos ter certeza de que não vamos atrapalhar o seu acesso. A qual servidor você está conectado?"

Jargão

TERMINAL BURRO Um terminal que não contém seu próprio microprocessador. Os terminais burros só aceitam comandos simples e exibem caracteres de texto e números.

"Como assim 'servidor'?", a pessoa perguntou.

"A qual computador você se conecta quando precisa pesquisar informações acadêmicas de alunos?"

A resposta foi admin.mu.edu e deu-lhe o nome do computador no qual os registros dos alunos estavam armazenados. Essa foi a primeira peça do quebra-cabeça: agora ele sabia qual era a sua máquina-alvo.

Digitou aquele URL no computador e não obteve resposta — como era de esperar, havia um firewall bloqueando o acesso. Assim sendo, executou um programa para saber se poderia se conectar a algum dos serviços que são executados naquele computador, e descobriu uma porta aberta com um serviço Telnet em execução, o qual permite que um computador se conecte remotamente a outro e o acesse como se fosse conectado diretamente usando um *terminal burro.* Ele agora só precisava ter acesso ao ID de usuário padrão e à senha.

Ele fez outra ligação para a secretaria, desta vez ouvindo com cuidado para ter certeza de que estava falando com uma pessoa diferente. Ele foi atendido por uma senhora e novamente disse ser do Centro de Computadores da universidade. Contou que estavam instalando um novo sistema de produção para os registros administrativos. Como um favor, ele gostaria que ela se conectasse ao sistema novo, ainda no modo de teste, para saber se ela conseguiria acessar os registros acadêmicos dos alunos. Ele deu a ela o endereço IP para a conexão e a orientou nesse processo.

Na verdade, o endereço IP levou até o computador no qual Michael estava sentado na biblioteca do *campus.* Usando o mesmo processo descrito neste capítulo, ele havia criado um simulador de login --- uma tela simulada de login — que se parecia com aquela que ela estava acostumada a ver quando entrava no sistema para acessar os registros dos alunos. "Não está funcionando", ela lamentou. "Ele fica dizendo 'Login incorreto'."

Nesse ponto o simulador de login havia passado as teclas digitadas com o seu nome de conta e senha para o terminal de Michael. Missão cumprida. Ele explicou a ela: "Ah, algumas das contas ainda não foram trazidas para esta máquina. Vou configurar a sua conta e ligo de volta." Tomando o cuidado de não deixar pontas soltas, como todo engenheiro social eficiente deve fazer, ele ligou mais tarde para dizer que o sistema de testes ainda não estava funcionando corretamente e, se ela permitisse, ele ou outro funcionário do Centro de Computadores ligaria para ela quando tivesse descoberto o que estava causando o problema.

O administrador prestativo

Agora Michael sabia de qual sistema de computadores precisava acessar e tinha um ID e uma senha de usuário. Mas quais comandos ele precisaria para pesquisar os arquivos com as informações sobre um formando em ciência da computação com o nome e a data de formatura certos? O banco de dados de alunos seria proprietário, criado no *campus* para atender aos requisitos específicos da universidade e da secretaria e teria uma forma exclusiva de ser acessado.

A primeira etapa para eliminar esse último empecilho seria descobrir quem poderia orientá-lo nos mistérios da pesquisa do banco de dados de alunos. Ligou novamente para a secretaria, desta vez falando com uma pessoa diferente. Contou que era da Diretoria de Engenharia e perguntou: Com quem podemos obter ajuda quando temos problemas para acessar os arquivos acadêmicos dos alunos?"

Minutos mais tarde ele estava ao telefone com o administrador do banco de dados da faculdade empregando o golpe da simpatia: "Meu nome é Mark Sellers, do escritório do Secretário. Sou novo aqui. Desculpe estar ligando para você, mas eles estão todos em uma reunião esta tarde e não há ninguém aqui para me ajudar. Preciso recuperar uma lista de todos os formandos em ciência da computação entre 1990 e 2000. Eles precisam disso até o final do dia e se eu não tiver a lista talvez não tenha este emprego por muito tempo. Você estaria disposto a ajudar um rapaz com problemas?" Ajudar as pessoas era algo que fazia parte do trabalho desse administrador de banco de dados, portanto, ele teve muita paciência ao falar com Michael e explicar o passo a passo do processo.

Quando desligaram, Michael tinha feito o download de toda a lista dos formandos em ciência da computação para aqueles anos. Em alguns minutos executou uma pesquisa, localizou dois Michael Parkers, escolheu um deles e obteve o número do seguro social da vítima, bem como outras informações pertinentes que estavam armazenadas no banco de dados.

Ele havia acabado de se tornar "Michael Parker, bacharel em Ciência da Computação, formado com louvor em 1998".

Analisando a trapaça

Esse ataque usou um truque do qual já falei antes: o atacante pedindo ao administrador de banco de dados de uma organização para orientá-lo nas etapas para a execução de um processo de computador que ele não sabia como executar. Uma virada poderosa e efetiva de mesa. equivalente a pedir ao dono de uma loja para ajudá-lo a transportar uma caixa contendo itens que você acabou de roubar das prateleiras e colocá-la no seu carro.

Recado do Mitnick

Os usuários de computadores às vezes não têm a menor pista das ameaças e vulnerabilidades associadas à engenharia social que existem no mundo da tecnologia. Eles têm acesso às informações, mas não têm o conhecimento detalhado daquilo que pode ser uma ameaça à segurança. Um engenheiro social visa um empregado que tem pouca compreensão de como são valiosas as informações que ele pode dar e, assim, fornecê-los a um estranho.

EVITANDO A TRAPAÇA

A simpatia, a culpa e a intimidação são três gatilhos psicológicos muito conhecidos usados pelo engenheiro social, e essas histórias demonstraram as táticas em ação. Mas o que você e a sua empresa podem fazer para evitar esses tipos de ataques?

Protegendo os dados

Algumas das histórias deste capitulo enfatizam o perigo de enviar um arquivo para alguém que você não conhece, mesmo quando aquela pessoa é (ou parece ser) um empregado e o arquivo está sendo enviado *internamente* para um endereço de correio eletrônico ou máquina de fax dentro da empresa.

A política de segurança da empresa precisa ser muito específica quanto às salvaguardas para proteger dados valiosos contra alguém que não seja conhecido pessoalmente como o remetente. Procedimentos exatos precisam ser estabelecidos para a transferência de arquivos que contêm informações confidenciais. Quando a solicitação vem de alguém que não se conhece pessoalmente, deve haver etapas claras para a verificação, com níveis diferentes de autenticação, dependendo do quanto essas informações sejam confidenciais.

Estas são algumas técnicas a serem levadas em conta:

- Estabelecer a necessidade de saber (a qual pode exigir a obtenção da autorização do proprietário designado das informações).
- Manter um registro pessoal ou departamental dessas transações.
- Manter uma lista das pessoas que foram treinadas especialmente nos procedimentos e que têm poderes para autorizar o envio das informações confidenciais. Exigir que apenas essas pessoas possam enviar as informações para alguém fora do grupo de trabalho.
- Se uma solicitação de dados for feita por escrito (e-mail, fax ou correio convencional), tomar cuidados adicionais para verificar se a solicitação realmente veio da pessoa da qual ela parece ter vindo.

Sobre as senhas

Todos os empregados que podem acessar informações confidenciais — e hoje isso significa quase todo empregado que usa um computador — precisam entender que atos simples, como trocar de senha, mesmo por alguns momentos, podem levar a grandes quebras da segurança.

O treinamento em segurança precisa abordar o tópico das senhas, que deve se concentrar em quando e como alterar a sua senha, o que constitui uma senha aceitável e os perigos de deixar que qualquer pessoa se envolva no processo. Particularmente, o treinamento precisa veicular para todos os empregados a necessidade de eles suspeitarem de *qualquer* solicitação que envolva suas senhas.

A principio isso parece ser uma mensagem simples para os empregados. Mas ela não é. Para que compreendam bem essa idéia é preciso que os empregados entendam como um ato de mudar uma senha pode levar a um comprometimento da segurança. Você pode dizer a uma criança para "olhar para os dois lados da rua ao atravessar", mas até ela entender porque isso é importante, você só depende da obediência cega. E as regras que exigem a obediência cega em geral são ignoradas ou esquecidas.

Observação

As senhas são um foco tão importante dos ataques da engenharia social que dedicamos uma seção separada no Capitulo 16 a elas. Lá você encontrará as políticas específicas recomendadas para o gerenciamento das senhas.

Um ponto central de apoio

A sua política de segurança deve estabelecer uma pessoa ou um grupo designado como um ponto central ao qual devem ser relatadas as atividades suspeitas que parecem ser tentativas de infiltração na sua organização. Todos os empregados precisam saber para quem devem ligar quando suspeitarem de uma tentativa de invasão eletrônica ou física. O número de telefone desse local sempre deve estar à mão para que os funcionários não tenham de procurar quando suspeitarem de que um ataque está ocorrendo.

Proteja a sua rede

Os empregados precisam entender que o nome de um servidor ou rede de computadores não é uma informação comum, mas sim uma informação que pode dar a um atacante o conhecimento essencial que o ajuda a ganhar a confiança ou encontrar a localização das informações que ele deseja.

Em particular, pessoas tais como os administradores de banco de dados, que trabalham com software, pertencem àquela categoria de pessoas que têm especialização técnica e que precisam operar sob determinadas regras especiais e bastante restritivas sobre a verificação da identidade das pessoas que ligam para elas para obter informações ou consultoria.

As pessoas que fornecem regularmente qualquer tipo de ajuda com computadores precisam estar bem treinadas sobre os tipos de solicitações que devem levantar suspeitas e sugerir que o interlocutor pode estar tentando realizar um ataque de engenharia social.

Vale a pena notar, porém, que, sob a perspectiva do administrador de banco de dados da última história deste capítulo, o interlocutor atendia aos critérios de ser um usuário legítimo: ele estava ligando do *campus* e obviamente estava em um site que requeria um nome de conta e uma senha. Isso só deixa claro mais uma vez a importância de ter procedimentos padronizados para a verificação da identidade de alguém que solicita informações, sobretudo em um caso como esse, no qual o interlocutor estava pedindo ajuda para obter acesso a registros confidenciais.

Tudo isso vale em dobro para faculdades e universidades. Não é novidade que o hacking de computadores é o passatempo preferido de muitos alunos da faculdade e também não deve ser surpresa que os registros dos alunos — e eventualmente os registros da faculdade também —- sejam um alvo tentador. Esse abuso é tão disseminado que algumas corporações consideram os *campi* como um ambiente hostil e criam regras de firewall que bloqueiam o acesso das instituições educacionais que têm endereços terminados em *.edu.*

O resultado disso tudo é que todos os registros de alunos e de pessoal de qualquer tipo devem ser vistos como alvos primários para um ataque, e devem ser bem protegidos como informações confidenciais.

Dicas de treinamento

A maioria dos ataques da engenharia social tem uma defesa ridiculamente fácil... para todos aqueles que sabem o que procurar.

Sob a perspectiva corporativa, o bom treinamento é fundamental. Mas também há a necessidade de algo mais: várias formas de *lembrar* as pessoas sobre aquilo que aprenderam.

Use telas chamativas que aparecem quando o computador do usuário é ligado, com uma mensagem de segurança diferente a cada dia. A mensagem deve ser criada para que não desapareça

automaticamente, e deve exigir que o usuário clique em algum tipo de confirmação de que ele leu a mensagem.

Outra abordagem que recomendo é iniciar uma série de lembretes de segurança. Os lembretes freqüentes são importantes. É preciso que haja um programa constante de conscientização. Os lembretes não devem ser escritos sempre da mesma forma. Estudos têm mostrado que essas mensagens são recebidas com mais eficiência quando a sua redação varia ou quando diferentes exemplos são usados.

Uma abordagem excelente é usar anúncios curtos nos newletteres da empresa. Esses anúncios não devem ser um artigo completo sobre o assunto, embora a coluna de segurança certamente seja valiosa. Em vez disso, crie um campo com duas ou três colunas de largura, algo como um pequeno anúncio no seu jornal local. Em cada edição, apresente um novo lembrete de segurança nessa forma curta para chamar a atenção dos leitores.

Capítulo 9

O Golpe Inverso

O *Golpe de Mestre,* filme mencionado em outra parte deste livro (e na minha opinião provavelmente o melhor filme que já foi feito sobre um golpe), descreve o seu enredo de truques com detalhes fascinantes. A operação do golpe no filme é uma descrição exata de como os principais estelionatários executam o "the wire", um dos três tipos de golpes chamados de "grandes golpes". Se você quer saber como uma equipe de profissionais consegue dar um golpe envolvendo uma grande soma em dinheiro em uma única noite, este é o melhor livro.

Mas os golpes tradicionais, sem levar em conta seus truques em particular, seguem um padrão. As vezes um golpe e dado ao contrário, o que é chamado *de golpe inverso.* Essa é uma inversão interessante, na qual o atacante cria uma situação para que a vítima peça ajuda ao *atacante,* ou um colega faz uma solicitação que é atendida pelo atacante.

Como isso funciona? Você vai descobrir em breve.

A ARTE DA PERSUASÃO AMISTOSA

Quando uma pessoa de nível intelectual médio cria o cenário de um ataque de computador, o que geralmente nos vem à mente é a imagem pouco louvável de um maluco solitário e introvertido, cujo melhor amigo é seu computador, e que tem dificuldades para conversar, exceto por meio de mensagens rápidas. O engenheiro social, o qual, via de regra, tem habilidades de hacker, também tem habilidades pessoais opostas — habilidades bem desenvolvidas para usar e manipular as pessoas que permitem que ele consiga as informações de forma que você nunca acreditaria que fosse possível.

O interlocutor de Angela

Local: Filial de Valley, Industrial Federal Bank.

Hora: 11 h27

Angela Wisnowski atendeu a ligação telefônica de um homem que dizia estar para receber uma herança considerável e queria informações sobre os diferentes tipos de contas de poupança,

Jargão

GOLPE INVERSO Um golpe no qual a pessoa atacada pede ajuda ao atacante.

certificados de depósito e outros investimentos que ela pudesse sugerir como seguros, mas com rendimentos decentes. Ela explicou que havia diversas opções e perguntou se ele não queria aparecer no banco para discutir os detalhes com ela. Ele disse que viajaria assim que o dinheiro chegasse e tinha muitas providencias para tomar. Assim sendo, ela começou sugerindo algumas possibilidades e dando os detalhes das taxas de juros, do que acontece se você vender um título antes e assim por diante e, ao mesmo tempo, tentava descobrir quais eram os seus objetivos de investimentos.

Ela parecia estar fazendo algum progresso quando ele afirmou: "Ah, sinto muito, preciso atender outra linha. Quando posso terminar a minha conversa com você para tomar algumas decisões? A que horas você sai para o almoço?" Ela contou que saia às 12h30 e ele disse que tentaria ligar de volta antes disso ou no dia seguinte.

O interlocutor de Louis

Os principais bancos usam códigos internos de segurança que mudam todos os dias. Quando alguém de uma filial precisa de informações de outra filial, ele prova que tem autorização para obter as informações demonstrando que conhece o código do dia. Para maior segurança e flexibilidade, alguns dos principais bancos usam diversos códigos todos os dias. Nesse local da Costa Oeste que chamarei de Industrial Federal Bank. cada empregado encontra todas as manhãs uma lista de cinco códigos para o dia. os quais são identificados com as letras A a E,

Local: o mesmo.

Hora: 12h48, naquele mesmo dia.

Louis Halpburn nem imaginava o que iria acontecer quando recebeu uma ligação naquela tarde, uma ligação como tantas outras que recebia várias vezes por semana.

"Alô", disse o Interlocutor. "Aqui é Neil Webster. Estou ligando da filial 3182 em Boston. Quero falar com Angela Wisnowski. por favor."

"Ela está em horário de almoço. Posso ajudar?"

"Bem, ela deixou uma mensagem pedindo para enviar um fax com algumas informações de um dos nossos clientes."

O interlocutor parecia ter tido um dia ruim.

"A pessoa que normalmente trata dessas solicitações está doente", ele prosseguiu. Tenho uma pilha delas aqui. são quase 4 da tarde e preciso sair para ir ao médico em meia hora."

A manipulação — dar todas as razões pelas quais a outra pessoa deve sentir pena dele — fazia pane da trama. Ele continuou "Não sei quem recebeu o recado dela pelo telefone, mas o número do fax está ilegível. É 213 alguma coisa. Qual é o resto do número?"

Louis deu o número do fax e o interlocutor disse: "Muito bem. obrigado. Antes que eu possa enviar este fax. preciso do Código B."

"Mas foi você que me ligou", ele salientou com tanta frieza que o homem de Boston entendeu a mensagem.

Isso é bom, o interlocutor pensou. *É bom quando as pessoas não caem na primeira tentativa. Se eles não resistem um pouco, o trabalho fica fácil demais e posso começar a ficar preguiçoso.*

Ele disse para Louis: "O problema é que tenho um gerente de filial aqui que ficou paranóico com essa história de verificar tudo o que enviamos. Mas ouça, se vocês não precisam do fax com as informações, tudo bem. Não é preciso verificar."

"Olhe", comentou Louis, "Angela volta em meia hora mais ou menos. Posso pedir para ela ligar para você de volta."

"Vou dizer para ela que não pude enviar as informações hoje porque você não conseguiu identificar essa solicitação como legítima dando-me o código. Se eu não estiver doente amanhã, ligo para ela de volta."

"Tudo bem."

"A mensagem diz 'Urgente'. Sem verificação estou de mãos atadas. Você diz para ela que tentei enviar as informações, mas você não pode me dar o código, OK?"

Louis não resistiu à pressão. Um suspiro audível de aborrecimento pôde ser ouvido no telefone.

"Bem", ele disse, "espere um pouco, tenho de ir até o meu computador. Qual código você queria?"

"O B", afirmou o interlocutor.

Ele colocou a ligação em espera e, em seguida, voltou à linha. "É 3184."

"Esse não é o código certo."

"Sim é ele — B é 3184."

"Eu não disse B, disse E."

"Ah, droga. Espere um pouco."

Outra pausa enquanto ele olhava novamente os códigos.

"E é 9697."

"9697 — certo. Já estou enviando o fax, OK?"

"Está bem, obrigado."

O interlocutor de Walter

"Industrial Federal Bank, Walter."

"Oi, Walter, aqui é Bob Grabowski da Studio City, filial 38", disse o interlocutor. "Preciso que você encontre um cartão de assinaturas de uma conta de cliente e o mande por fax para mim."

O cartão de assinaturas tem mais do que apenas a assinatura do cliente. Ele também tem informações de identificação, itens conhecidos, tais como o número do seguro social, a data de nascimento, o nome de solteira da mãe e eventualmente até mesmo o número da carteira de motorista. Ele é muito útil para um engenheiro social.

"Tudo bem. Qual é o Código C?"

"Outro caixa está usando o meu computador agora", explicou o interlocutor. "Mas acabei de usar o B e o E e lembro deles. Me peça um deles."

"Muito bem, qual é o E?"

"O E é 9697."

Alguns minutos depois, Walter enviou por fax o cartão de assinaturas solicitado.

O interlocutor de Donna Plaice

"Oi, aqui é o Sr. Anselmo."

"Posso ajudar?"

"Para qual número 800 ligo quando quero saber se um depósito já foi compensado?"

"O sr. é cliente do banco?"

"Sim, e não uso esse número há algum tempo e não sei onde o anotei."

"O número é 800-555-8600."

"OK, obrigado."

A história de Vince Capelli

Filho de um policial das ruas de Spokane, Vince sabia desde pequeno que não ia passar a sua vida trabalhando como um escravo e arriscando o pescoço para ganhar salário mínimo. Seus dois principais objetivos eram sair de Spokane e abrir um negócio próprio. As piadas dos seus colegas durante toda a faculdade só o incentivavam mais — eles achavam hilariante o fato de ele estar tão envolvido em começar seu próprio negócio, mas não ter a menor idéia da área na qual queria atuar.

No fundo Vince sabia que eles estavam certos. A única coisa que fazia bem era ser apanhador no time de beisebol da faculdade. Mas não era bom o suficiente para conseguir uma bolsa de estudos, já que não era bom para o beisebol profissional. Assim sendo, em que área iniciaria o seu negócio?

Havia uma coisa da qual os amigos de Vince nunca se deram conta: tudo que um deles tinha — fosse um canivete novo, um par de luvas de frio, uma nova namorada sexy —, se Vince admirasse essa coisa, em pouco tempo ele a tinha. Ele não a roubava nem se esgueirava pelas costas de ninguém. A pessoa que tinha aquilo que ele queria dava-lhe de livre e espontânea vontade. Nem mesmo Vince sabia como fazia isso: ele não conhecia a si mesmo. As pessoas simplesmente pareciam deixar que ele conseguisse o que quisesse.

Vince Capelli era um engenheiro social desde tenra idade, embora nunca tivesse ouvido falar do termo.

Seus amigos pararam de rir quando se formaram na faculdade. Enquanto os outros percorriam a cidade procurando empregos onde tinham de dizer "Você quer com batata frita?", o pai de Vince o mandou falar com um velho colega policial que havia deixado a corporação para iniciar o próprio negócio de investigações particulares em São Francisco. Ele rapidamente reconheceu o talento de Vince para o trabalho e o contratou.

Isso aconteceu há seis anos. Ele odiava a parte de conseguir os bens das esposas infiéis, a qual envolvia horas aborrecidas sentado e observando, mas sentia-se continuamente desafiado quando precisava desencavar as informações de bens para os advogados que tentavam descobrir se algum miserável era suficientemente rico para valer uma ação. Essas tarefas davam-lhe muitas chances de usar a sua esperteza.

Uma dessas chances foi quando teve de investigar as contas bancárias de um cara chamado Joe Markowitz. Joe teria trabalhado em um negócio duvidoso com um ex-amigo seu. Agora esse amigo queria saber se, em caso de um processo. Markowitz teria dinheiro suficiente para devolver pelo menos parte do seu dinheiro.

A primeira etapa que Vince teria de executar seria descobrir pelo menos um, mas de preferência dois códigos de segurança do banco naquele dia. Isso parece um desafio quase impossível: o que levaria um empregado de banco a burlar o seu próprio sistema de segurança? Pergunte a si mesmo — se quisesse fazer isso. você teria alguma idéia do lugar por onde deveria começar?

Para as pessoas como Vince isso é muito fácil.

As pessoas confiam quando você conhece a linguagem interna de seus trabalhos e de suas empresas. Isso é como mostrar que você pertence ao seu circulo interno. Isso é como um aperto de mão secreto.

Eu não precisava de muita coisa para realizar uma tarefa com essa. Definitivamente isso não e como uma cirurgia de cérebro. Eu só precisava de um número de filial. Quando liguei para o escritório de Beacon Street, em Búfalo, a pessoa que atendeu o telefone parecia ser um caixa.

"Aqui é Tim Ackerman", eu disse. Qualquer nome servia, ele não ia anotar o nome mesmo. "Qual é o número da sua filial?"

"O número do telefone ou o número da filiai?", ele quis saber, o que parecia estúpido, porque eu havia acabado de discar para o número de telefone, não havia?

"O número da filial."

"3182", ele respondeu. Simples assim. Sem perguntas do tipo "Para que você quer saber?" ou algo parecido. Porque essas não são informações confidenciais, elas estão escritas em quase todos os documentos que se usam.

Etapa dois, ligar para a filial onde o meu alvo fazia suas transações bancárias, obter o nome de um de seus funcionários e descobrir quando a pessoa estaria em hora de almoço. Angela. Ela sai às I2h30. Até aqui tudo bem.

Etapa três, ligar de volta para a mesma filial durante o horário de almoço de Angela, dizer que estou ligando do número de filial "tal" em Boston, que Angela precisa que eu envie essas informações, e que eles me dêem o código do dia. Essa é a parte mais complicada. Se eu estivesse fazendo um teste para ser um engenheiro social, colocaria algo desse tipo no teste, um lugar onde a vítima começasse a suspeitar —e com bons motivos — e você ainda teria de ficar lá até dobrá-la e obter as informações necessárias. Você não pode fazer isso recitando linhas de um script ou rotina de aprendizado, você precisa ler a sua vítima, entender o seu estado de espírito, enganá-la como se engana um peixe dando um pouco de linha e puxando, mais um pouco de linha e puxando. Até você pegá-lo na rede e jogá-lo no barco!

Foi assim que o enganei e consegui os códigos do dia. Uma grande etapa. Na maioria dos bancos. eles usam apenas um código e eu estaria a salvo. O Industrial Federal Bank usa cinco códigos e, portanto, ter apenas um entre cinco não significa muita coisa. Com dois em cinco, eu teria muito mais chances de passar para o próximo ato do pequeno drama. Amo essa parte onde digo "Eu não disse B, disse E". Quando funciona, é lindo. E na maior parte do tempo funciona.

Se eu conseguisse um terceiro seria melhor ainda. Na verdade, conseguiria obter até três em uma única ligação — "B", "D" e "E" são tão parecidos que você pode dizer que eles não entenderam de

novo. Mas você precisa estar falando com alguém que seja verdadeiramente lento. E esse homem não era. Assim, fiquei com os dois códigos.

Os códigos do dia seriam o meu trunfo para obter o cartão de assinaturas. Ligo e o atendente pede um código. Ele quer o C, e eu só tenho o B e o E. Mas isso não é o fim do mundo. Você precisa permanecer calmo em um momento como esse, deve parecer confiante, continuar com o plano. Eu o enganei com a história de que "Alguém está usando o meu computador, peça um destes outros".

Todos somos empregados da mesma empresa, estamos todos nisso juntos, vê se facilita para mim, cara — é isso que você espera que a vítima esteja pensando em um momento como esse. E ele seguiu o script direitinho. Ele aceitou uma das opções que ofereci, dei a resposta certa, ele enviou o fax do cartão de assinaturas.

Eu já estava quase lá. Mais uma ligação me deu o número 800 que os clientes usam para o serviço automatizado no qual uma voz eletrônica lê as informações que você pede. Com o cartão de assinaturas, eu tinha todos os números de contas do meu alvo e seus números de identificação, porque aquele banco usava os cinco primeiros ou os quatro últimos dígitos do número do seguro social. De canela em punho liguei para o número 800 e após alguns minutos apertando botões, tinha o saldo mais recente em todas as quatro contas do indivíduo, e só por medida de segurança os seus depósitos mais recentes e as retiradas feitas sobre cada um deles.

Tudo aquilo que o meu cliente havia pedido e mais. Sempre gosto de fornecer um extra para os clientes. Isso os mantêm felizes. Afinal de contas, são os negócios repetidos que mantêm uma operação em funcionamento, certo?

Analisando a trapaça

O segredo de todo esse episódio foi a obtenção dos importantes códigos do dia, e para fazer isso o atacante, Vince, usou diversas técnicas diferentes.

Ele começou com um pouco de queda de braço verbal quando Louis relutou em dar-lhe um código. Louis estava certo em relutar—os códigos foram criados para serem usados na direção oposta. Ele sabia que em um fluxo normal de coisas, o interlocutor desconhecido começaria dando-lhe um código de segurança. Esse era o momento crítico para Vince, o gancho do qual dependia todo o sucesso desse esforço.

Diante das suspeitas de Louis, Vince simplesmente usou a manipulação, um apelo para a simpatia ("ir ao médico"), a pressão ("Tenho uma pilha de coisas para fazer e já são quase quatro horas") e a manipulação ("Diga a ela que você não quis me dar o código").

De forma inteligente, Vince não ameaçou realmente, ele apenas deixou uma ameaça implícita: Sc você não me der o código de segurança, não vou enviar as informações de cliente que a sua colega precisa e vou dizer a ela que eu queria enviar, mas que você não cooperou.

Mesmo assim, não sejamos apressados em culpar Louis. Afinal de contas, a pessoa que estava no telefone sabia (ou pelo menos *parecia* saber) que a colega Angela havia solicitado um fax. O interlocutor sabia sobre os códigos de segurança e sabia que eles eram identificados por letras. Ele disse que o seu gerente de filial estava pedindo o código para ter mais segurança. Isso não parecia uma razão verdadeira para não dar a ele a verificação que estava pedindo.

Louis não está sozinho. Os empregados do banco dão os códigos de segurança para os engenheiros sociais todos os dias. Isso é incrível, mas é verdadeiro.

Há uma linha indefinida na qual as técnicas de um detetive particular param de ser legais e começam a ser ilegais. Vince permaneceu legal até obter o número da filial. Ele até permaneceu legal

quando enganou Louis para lhe dar dois dos códigos de segurança do dia. Ele cruzou a linha quando obteve via fax as informações confidenciais de um cliente do banco.

Mas para Vince e seu empregador, esse é um crime de baixo risco. Quando você rouba dinheiro ou bens. alguém vai notar que eles desapareceram. Quando você rouba informações, na maior parte do tempo ninguém notará porque as informações ainda estão em seu poder.

Recado do Mitnick

Os códigos de segurança verbais são equivalentes às senhas, pois fornecem um meio conveniente e confiável de proteger os dados. Mas os empregados precisam conhecer os truques que os engenheiros sociais usam e devem ser treinados para não revelar os segredos de estado.

FAZENDO OS DETETIVES DE BOBOS

Para um detetive particular ou engenheiro social, quase sempre há ocasiões em que seria útil ter o número da carteira de motorista de alguém — por exemplo, se você quiser assumir a identidade de outra pessoa para obter informações sobre seus saldos bancários.

Além de bater a carteira da pessoa ou espiar sobre seus ombros em um momento oportuno, descobrir o número da carteira de motorista seria algo próximo do impossível. Mas para alguém que tenha habilidades de engenharia social, mesmo que modestas, isso dificilmente é um desafio.

Um engenheiro social em particular — Eric Mantini, como vou chamá-lo, precisava conseguir o número de carteira de motorista e os números de registro de veículo freqüentemente. Eric calculou que não era preciso aumentar o seu risco e ligar para o Departamento de Trânsito, passando sempre o mesmo golpe quando precisava daquelas informações. Ele se perguntava se não havia um modo de simplificar esse processo.

Provavelmente ninguém jamais havia pensado nisso antes, mas ele descobriu um modo de obter as informações num instante, sempre que as queria. Ele fez isso aproveitando-se de um serviço fornecido pelo Departamento de Trânsito do seu estado. Os Departamentos de Trânsito de muitos estados tomam as informações de acesso privilegiado sobre os cidadãos disponíveis para as empresas seguradoras, os detetives particulares e determinados outros grupos, os quais, de acordo com a lei foram considerados como tendo direito a elas pelo bem do comércio e da sociedade em geral.

Obviamente, o Departamento de Trânsito tem as limitações apropriadas para os tipos de dados que serão divulgados. A indústria dos seguros pode obter determinados tipos de informações dos arquivos, mas não outras. Um conjunto diferente de limitações aplica-se aos detetives e assim por diante.

Em geral, para os agentes da lei uma regra diferente é aplicada. O Departamento de Trânsito fornece as informações que estão em seus registros para qualquer juiz de direito que se identifique da maneira apropriada. No estado em que Eric morava na época, a identificação requerida era um Código do Solicitante emitido pelo Departamento de Trânsito, juntamente com o número da Carteira de Motorista do oficial. O empregado do Departamento de Trânsito sempre teria de comparar o nome do oficial com o número da sua Carteira de Motorista e com mais alguma informação — em geral a data de nascimento — antes de fornecer as informações.

O que o engenheiro social Eric queria fazer nada mais era do que se fazer passar por um oficial da lei.

Como ele conseguiu fazer isso? Pregando um golpe inverso nos policiais!

O golpe de Eric

Primeiro ele ligou para o número de informações da companhia telefônica e pediu o número de telefone da sede do Departamento de Trânsito na sede do governo estadual. Ele recebeu o número 503-555-5000, o qual, obviamente, é o número para as ligações do público em geral. Em seguida. ligou para o posto policial mais próximo e pediu para falar com a sala do teletipo — o escritório no qual as comunicações são enviadas e recebidas das outras polícias, do banco de dados nacional de crimes, das prisões locais e assim por diante. Assim que conseguiu falar com a sala de teletipo, ele disse que estava procurando o número de telefone da polícia para o qual teria de ligar ao falar com a sede estadual do Departamento de Trânsito.

"Quem é você?", perguntou o oficial de polícia da sala de teletipo.

"Aqui é o Al. Eu estava ligando para o 503-555-5753", ele disse. Isso era em parte uma suposição e em parte um número que ele tirou do nada; com certeza o escritório especial do Departamento de Trânsito que recebia ligações sobre a aplicação da lei deveria ter o mesmo código de área do número dado para o público ligar, e era quase certo que os próximos três dígitos, o prefixo, também fossem iguais. Tudo o que ele realmente precisava descobrir eram os quatro últimos dígitos.

A sala de teletipo do delegado não recebe ligações do público. E o interlocutor já tinha a maior parte do número. Obviamente essa era uma solicitação legitima.

"O número é 503-555-6127", respondeu o oficial.

Dessa forma, Eric agora tinha o número de telefone especial que os policiais usavam para ligar para o Departamento de Trânsito. Mas um número apenas não bastava para satisfazê-lo; o escritório deveria ter muito mais do que uma única linha telefônica e Eric precisava saber quantas linhas havia e o número de cada uma delas.

A central telefônica

Para executar seu plano ele precisava acessar a central telefônica que tratava das linhas telefônicas entre a polícia e o Departamento de Trânsito. Ele ligou para o Departamento de Telecomunicações estadual e disse que era da Nortel, o fabricante do DMS-100, uma das centrais telefônicas comerciais mais usadas. Ele perguntou: "Você pode me transferir para um dos técnicos em centrais telefônicas que trabalha com o DMS 100?"

Quando o técnico atendeu, ele afirmou ser do Centro de Suporte à Assistência Técnica da Nortel, no Texas, e explicou que eles estavam criando um banco de dados master para atualizar todas as centrais telefônicas com as atualizações de software mais recentes. Tudo seria feito remotamente — não seria necessária a participação de nenhum técnico. Mas eles precisam do número de discagem da central telefônica para executarem as atualizações diretamente do Centro de Suporte.

Isso parecia plausível e o técnico deu a Eric o número do telefone. Agora ele podia discar diretamente para uma das centrais telefônicas do estado.

Com segurança contra estranhos, as centrais telefônicas comerciais desse tipo têm uma senha, como qualquer outra rede de computadores corporativa. Todo bom engenheiro social com um histo-

rico de invasão por telefone sabe que as centrais telefônicas da Nortel fornecem um nome de conta default para as atualizações de software: os NTAs (abreviatura de Nortel Technical Assistance Support; nada sutil não é?). Mas e a senha? Eric discou várias vezes e cada vez tentava uma das opções mais óbvias e mais utilizadas. Inserir o mesmo nome da conta, NTAS, nada adiantou. Nem "helper", e também nem "patch".

Em seguida, tentou "atualização"... e conseguiu. Isso é típico. O uso de uma senha óbvia e que pode ser adivinhada facilmente é apenas melhor do que não ter nenhuma senha.

Isso agilizou o processo. Eric talvez soubesse tanto sobre aquela central telefônica e sobre como programar e solucionar os problemas quanto o técnico. Depois que conseguiu acessar a central telefônica como usuário autorizado, ele podia ter controle completo sobre as linhas telefônicas que eram o seu alvo. Do computador ele consultava a centra! telefônica do número de telefone que ele havia conseguido para as chamadas da polícia do Departamento de Trânsito, o número DMV, 555-6127. Ele descobriu que havia 19 outras linhas telefônicas no mesmo departamento. Obviamente, elas recebiam um volume alto de ligações.

Para cada ligação recebida, a central telefônica estava programada para "caçar" nas 20 linhas até encontrar uma que não estava ocupada.

Ele pegou a linha de número 18 da seqüência e digitou o código que incluía o encaminhamento de chamada para aquela linha. Com o número para o encaminhamento de chamadas, ele digitou o número do telefone do seu novo e barato telefone celular pré-pago, do tipo que os traficantes de drogas gostam, porque são baratos e podem ser jogados fora depois que o trabalho é executado.

Agora com o encaminhamento de chamadas ativado para a linha 18, assim que o escritório ficava cheio com 17 ligações em andamento, a próxima ligação a chegar não tocaria no escritório do Departamento de Trânsito, mas seria encaminhada para o telefone celular de Eric. Ele sentou e esperou.

Uma ligação para o Departamento de Trânsito

Logo depois das 8 horas daquela manhã o telefone celular tocou. Essa era a melhor parte e a mais deliciosa. Aqui estava Eric, o engenheiro social falando com um policial, alguém com autoridade para ir lá e prendê-lo ou conseguir um mandado de busca para encontrar evidências contra ele.

E não apenas um policial ligou, mas sim uma fileira deles, um após o outro. Em uma ocasião. Eric estava sentado em um restaurante almoçando com amigos, recebendo uma ligação a cada cinco minutos, escrevendo as informações em um guardanapo de papel e usando uma caneta emprestada. Até hoje ele acha isso muito engraçado.

Mas falar com os policiais não perturba um bom engenheiro social de maneira alguma. Na verdade, a emoção de enganar esses agentes da lei provavelmente aumentou o contentamento de Eric com a façanha.

De acordo com Eric, as ligações eram mais ou menos assim:

"Departamento de Trânsito, posso ajudar?"

"Aqui é o Detetive Andrew Cole."

"Oi. detetive. Como posso ajudá-lo?"

"Preciso de um Soundex na carteira de motorista 005602789", ele dizia, usando o termo familiar na polícia para pedir uma foto — o que é útil, por exemplo, quando os oficiais vão prender um suspeito e querem saber como ele é.

"É claro, deixe-me pegar a ficha", Eric respondia. "Detetive Cole, qual é o seu distrito?"

"Jefferson County". Em seguida, Eric fazia as perguntas mais importantes: "Detetive, qual é o seu código de solicitante?" "Qual é o número da sua carteira de motorista?" "Qual é sua data da nascimento?"

O interlocutor dava as suas informações de identificação pessoal. Eric fingia estar verificando as informações e depois dizia que as informações de identificação haviam sido confirmadas e pedia os detalhes sobre aquilo que o interlocutor queria do Departamento de Trânsito. Ele fingia começar procurando o nome, o interlocutor o ouvia digitando e, em seguida, dizendo algo do tipo "Ah, droga, meu computador deu pane novamente. Desculpe detetive, mas o meu computador está com problemas a semana toda. Você poderia ligar novamente e pedir para outro operador ajudá-lo?"

Dessa forma encerrava a ligação sem levantar nenhuma suspeita sobre o motivo pelo qual ele não pôde ajudar o oficial e atender à sua solicitação. Nesse meio tempo, Eric já tinha uma identidade roubada — os detalhes com os quais podia obter as informações confidenciais do Departamento de Trânsito sempre que precisasse.

Após atender as ligações durante algumas horas e obter dezenas de códigos de solicitante, Eric discava para a central telefônica e desativava o encaminhamento de chamadas. Durante meses depois disso, ele realizou trabalhos que lhes eram passados por empresas de investigação particular legítimas, as quais não queriam saber como ele obtinha as informações. Sempre que precisava, ele discava de novo para a central telefônica, ligava o encaminhamento de chamadas e coletava outra pilha de credenciais de policiais.

Analisando a trapaça

Vamos rever os golpes que Eric usou para realizar o seu trabalho. Na primeira etapa bem-sucedida, ele conseguiu que um delegado de uma sala de teletipo desse o número confidencial do Departamento de Trânsito para alguém totalmente estranho, aceitando o homem como um delegado sem solicitar nenhuma verificação.

Recado do Mitnick

Se você tiver uma central telefônica em sua empresa, o que a pessoa encarregada faria se recebesse uma ligação de um fornecedor pedindo o número de discagem? E, por falar nisso, essa pessoa já alterou a senha default da central? Essa senha é uma palavra fácil que pode ser encontrada em qualquer dicionário?

Em seguida, alguém do Departamento de Telecomunicações do estado fazia a mesma coisa, aceitando a alegação de Eric de que ele era o fabricante do equipamento e fornecendo ao estranho um número de telefone para discar para a central telefônica que atendia o Departamento de Trânsito.

Em grande parte, Eric conseguiu entrar na central telefônica por causa das práticas ruins de segurança implantadas pelo fabricante da central telefônica ao usar o mesmo nome de conta em todas as suas centrais. Essa falta de cuidado tornou muito fácil para o engenheiro social adivinhar a senha, sabendo mais uma vez que os técnicos das centrais telefônicas, assim como quase todas as outras pessoas, preferem as senhas mais fáceis de decorar.

Com o acesso à central telefônica, ele configurou o encaminhamento de chamadas de uma das linhas telefônicas da polícia do Departamento de Trânsito para o seu telefone celular.

Em seguida, na parte mais espalhafatosa, enganou um agente da lei após o outro para que eles revelassem não apenas os seus códigos de solicitante, como também suas próprias informações de identificação pessoal, dando a Eric a capacidade de se fazer passar por eles.

Embora, sem dúvida, um certo conhecimento técnico tivesse sido necessário para realizar essa façanha, isso poderia não ter funcionado sem a ajuda de uma série de pessoas que não tinham a menor idéia de que estavam falando com um impostor.

Essa história é outra ilustração do fenômeno no qual as pessoas não perguntam "Por que eu?". Por que o oficial do teletipo deu essas informações para algum representante de delegado que ele nem conhecia — ou, neste caso, um estranho *se fazendo passar* pelo representante do delegado — em vez de sugerir que ele obtivesse as informações de um colega representante ou do seu próprio oficial? Novamente, a única resposta que posso dar é que as pessoas raramente fazem essa pergunta. Não lhes ocorre perguntar? Elas não querem parecer tolas e pouco dispostas a ajudar? Talvez sim. Qualquer outra explicação seria pura adivinhação. Mas os engenheiros sociais não se importam com o motivo; eles só se importam com o fato de esse pequeno detalhe facilitar a obtenção das informações que, de outra forma, seriam difíceis de obter.

EVITANDO A TRAPAÇA

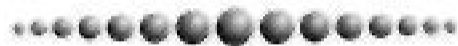
Um código de segurança bem utilizado agrega uma camada valiosa de proteção. Um código de segurança mal usado pode ser pior do que nenhum código, porque ele dá a ilusão de segurança quando ela na verdade não existe. Para que servem os códigos se os seus empregados não os mantêm em segredo?

Qualquer empresa que tenha necessidade de códigos verbais de segurança precisa declarar expressamente para seus empregados quando e como os códigos devem ser usados. Se fosse treinado adequadamente, o personagem da primeira história deste capítulo não teria de depender dos seus instintos, os quais foram facilmente superados, quando lhe foi pedido que desse um código de segurança para um estranho. Ele sentiu que naquelas circunstâncias o código não seria pedido, mas sem uma política clara de segurança — e sem o bom senso — ele o deu com facilidade.

Os procedimentos de segurança também devem definir as etapas a serem seguidas quando um empregado faz uma solicitação inadequada por um código de segurança. Todos os empregados devem ser treinados para relatar imediatamente qualquer solicitação de credenciais de autenticação, tais como o código diário ou uma senha, solicitação essa que é feita em circunstâncias suspeitas. Eles também devem informar quando uma tentativa de verificação da identidade de um solicitando não confere.

No mínimo, o empregado deve registrar o nome, o número do telefone e o escritório ou departamento do solicitante e depois desligar. Antes de ligar de volta, ele deve verificar se a organização realmente tem um empregado com aquele nome e se o número de telefone que ele deu coincide com o número da lista on-line ou impressa da empresa. Na maior parte do tempo, essa tática simples será o necessário para verificar se o interlocutor é quem diz ser.

A verificação torna-se um pouco mais complicada quando a empresa tem uma lista telefônica publicada em vez de uma versão on-line. As pessoas são contratadas, vão embora, mudam de departamentos, de cargos e de números de telefone. A lista de telefones impressa já está desatualizada no

dia seguinte à sua publicação, mesmo antes de ser distribuída. Mesmo as listas on-line nem sempre são confiáveis, porque os engenheiros sociais sabem como modificá-las. Se um empregado não puder verificar o número de telefone de uma fonte independente, ele deve ser instruído para verificar por outros meios, tais como entrar em contato com o gerente do empregado.

parte 3

Alerta de Invasão

Capítulo 10

Entrando nas Instalações

Por que é tão fácil para um estranho assumir a identidade do empregado de uma empresa e se fazer passar por ele de forma tão convincente que até mesmo as pessoas que são altamente preocupadas com a segurança são enganadas? Por que é tão fácil enganar indivíduos que têm conhecimento total dos procedimentos de segurança, pessoas que suspeitam das outras pessoas que não conhecem pessoalmente e que protegem os interesses de suas empresas?

Pense nessas perguntas ao ler as histórias deste capítulo.

O GUARDA DE SEGURANÇA COM PROBLEMAS

Data/Hora: terça-feira, 17 de outubro, 2hl6.

Local: Skywatcher Aviation, Inc., fábrica nas vizinhanças de Tucson, Arizona.

A história do guarda de segurança

Ouvir o barulho dos seus saltos de couro batendo no chão enquanto caminhava nos corredores da fábrica quase deserta era algo que fazia Leroy Greene sentir-se muito melhor do que quando tinha de passar a noite de vigília na frente dos monitores de vídeo do escritório da segurança. Lá ele não podia fazer nada além de ficar olhando as telas, nem podia ler uma revista ou a sua Bíblia com capa de couro. Ele tinha de ficar sentado olhando os monitores com imagens paradas, nas quais quase nada se movia.

Mas ao caminhar pelos corredores, pelo menos estava esticando as pernas, e, quando se lembrava, abria os braços e movia os ombros durante a caminhada, fazendo assim um pouco de exercício. Entretanto, isso não contava como exercício para um homem que havia jogado na equipe de futebol americano All-City, no ginásio. Mesmo assim, ele pensava, trabalho é trabalho.

Ele virou o corredor para o sudoeste e começou a percorrer a galeria, supervisionando a área de produção de 800 m de comprimento. Ele olhou para baixo e viu duas pessoas caminhando após a linha de helicópteros parcialmente montados. Elas pararam e pareciam apontar algumas coisas. Uma visão estranha nessa hora da madrugada. "É melhor eu verificar", ele pensou.

Leroy foi até a escada que o levaria à linha de produção atrás das pessoas, e elas não o viram até que chegou ao seu lado. "Bom-dia. Posso ver seus crachás, por favor?", ele perguntou. Leroy sempre tentava manter a voz suave nesses momentos; ele sabia que o seu tamanho avantajado poderia parecer ameaçador.

"Oi, Leroy", um deles respondeu, lendo o nome no seu crachá. "Sou Tom Stilton, do escritório de Marketing em Fênix. Vim para algumas reuniões na cidade e queria mostrar para o meu amigo como os maiores helicópteros do mundo são construídos."

"Sim, senhor. O seu crachá, por favor", repetiu Leroy. Ele não pôde deixar de notar como eles eram jovens. O rapaz do marketing parecia haver saído do colégio, o outro tinha o cabelo pelo ombro e parecia ter uns 15 anos.

O rapaz de cabelo cortado procurou o crachá em um bolso e. em seguida, começou a procurar nos outros bolsos. De repente, Leroy começou a ter um mau pressentimento sobre isso tudo. "Droga", disse o rapaz. "Devo ter deixado no carro. Vou lá pegar — me dê dez minutos para ir até o estacionamento e voltar."

Leroy já estava com a sua prancheta. "Qual era mesmo o seu nome, senhor?", ele perguntou e anotou a resposta com cuidado. Em seguida, pediu que eles fossem com ele até o Escritório da Segurança. No elevador para o terceiro andar, Tom explicou que estava na empresa há apenas seis meses e esperava que isso não lhe trouxesse problemas.

Na sala de monitoramento da Segurança, os dois outros seguranças do turno da noite de Leroy juntaram-se a ele para fazer perguntas ao par. Stilton deu seu número de telefone e disse que a sua chefe era Judy Underwood e deu o número do telefone dela, e todas as informações foram checadas no computador. Leroy afastou-se com os dois outros seguranças e conversaram sobre o que fazer. Ninguém queria fazer a coisa errada; todos os três concordaram que era melhor ligar para o chefe do rapaz, embora isso significasse acordá-la no meio da noite.

Leroy ligou ele mesmo para a Sra. Underwood, explicou quem ele era e perguntou se o Sr. Tom Stilton trabalhava para ela. Parecia que ela estava meio adormecida ainda. "Sim", ela disse.

"Bem, o encontramos aqui na linha de produção às 2h30 da manhã sem nenhum crachá de identificação."

A Sra. Underwood pediu: "Deixe-me falar com ele."

Stilton pegou o telefone e disse: "Judy, sinto muito que os seguranças te acordaram no meio da noite. Espero que você não fique zangada comigo por causa disso."

Ele ouviu e depois continuou: "Acontece que eu tinha de estar aqui de manhã de qualquer maneira para aquela reunião sobre o novo press release. De qualquer forma, você recebeu o e-mail sobre o acordo com o Thompson? Precisamos nos reunir com o Jim na segunda-feira de manhã para não perdermos esse negócio. E ainda tenho aquele almoço com você na terça-feira, certo?"

Ele ouviu mais um pouco, disse adeus e desligou.

Isso pegou Leroy de surpresa. Ele pensou que voltaria ao telefone para que a senhora lhe dissesse que estava tudo bem. Ele se perguntava se deveria ligar novamente para ela, mas pensando melhor achou que não. Ele já a havia incomodado no meio da noite. Se ele ligasse novamente, ela poderia ficar aborrecida e iria reclamar com o chefe dele. *"Por que criar caso?"*, ele refletiu.

"Tudo bem se eu mostrar ao meu amigo o restante da linha de produção?", Stilton perguntou a Leroy. "Você quer vir junto para nos vigiar?"

"Vá em frente", afirmou Leroy. "Olhe tudo. Só não esqueça o crachá da próxima vez. E avise a Segurança antes de precisar estar na fábrica fora do horário de trabalho — esse é o regulamento."

"Vou me lembrar disso, Leroy", disse Stilton. E eles foram embora.

Menos de dez minutos depois o telefone tocou no Escritório da Segurança. Era a Sra. Underwood na linha. "Quem era aquele rapaz?", ela queria saber. Ela disse que tentou fazer perguntas, mas ele ficava falando sobre um almoço que tinha com ela e ela não sabia quem era ele.

Os seguranças ligaram para a recepção e para o guarda do portão do estacionamento. Ambos disseram que os dois jovens haviam saído fazia alguns minutos.

Mais tarde, ao contar a história, Leroy sempre terminava dizendo: "Meu Deus, o meu chefe queria acabar comigo. Eu tenho sorte de ainda ter o emprego."

A história de Joe Harper

Só para ter idéia do que poderia fazer, o jovem Joe Harper de 17 anos vinha se esgueirando e entrando em prédios há mais de um ano, ora durante o dia, ora à noite. Filho de um músico e uma garçonete, ambos trabalhando no turno da noite, Joe ficava muito tempo sozinho. A sua história para aquele mesmo incidente nos dá pistas instrutivas sobre como tudo aconteceu.

Tenho esse amigo, o Kenny, que acha que quer ser um piloto de helicópteros. Ele me pediu para levá-lo até a fábrica Skywatcher e ver a linha de produção dos helicópteros. Ele sabe que já entrei em outros lugares antes. Infiltrar-se em lugares nos quais não deveria estar requer uma overdose de adrenalina.

Mas você simplesmente não entra em uma fábrica ou um prédio de escritórios. E preciso pensar muito antes, planejar muito e fazer um trabalho grande de reconhecimento do alvo. Você tem de verificar na página Web da empresa os nomes e cargos, a estrutura hierárquica e os números de telefone. É preciso também ler recortes de jornais e artigos de revistas. Ser meticuloso é a minha precaução para que eu possa falar com qualquer pessoa que me desafie com tanto conhecimento quanto o de qualquer empregado.

Por onde começar, então? Em primeiro lugar, procurei na Internet para saber onde a empresa tinha escritórios e vi que a sede corporativa era em Fênix. Perfeito. Liguei e pedi para falar com o Marketing; toda empresa tem um departamento de marketing. Uma senhora atendeu e eu disse que era da Blue Pencil Graphics e queria saber se eles teriam interesse em usar os nossos serviços e com quem poderia falar. Ela disse que eu deveria falar com Tom Stilton. Pedi o número do seu telefone e ela respondeu que eles não davam essas informações, mas que ela poderia me passar para ele. A ligação caiu no voice mail, e a sua mensagem dizia: "Aqui é Tom Stilton, de Gráficos, ramal 3147. por favor deixe a sua mensagem". E claro que eles não dão os ramais, mas esse funcionário deixa o seu ramal bem no seu voice mail. Isso era ótimo. Agora eu tinha um nome e um ramal.

Fiz outra ligação para o mesmo escritório. "Olá, eu estava procurando por Tom Stilton. Ele não está. Gostaria de fazer uma perguntinha ao chefe dele." O chefe estava fora também, mas quando desliguei, eu já tinha o nome do chefe. E ele também havia educadamente deixado o seu ramal no voice mail.

Provavelmente eu poderia passar pelo guarda da recepção sem esforço, mas eu já havia passado por aquela fábrica e acho que me lembrava de que havia uma cerca ao redor do estacionamento. Uma cerca significa um guarda que verifica a sua identidade quando você tenta entrar de carro. Naquela noite, eles poderiam estar tomando nota dos números das placas dos carros também e eu teria de comprar uma placa antiga em um ferro-velho.

Mas primeiro eu teria de obter o número de telefone da guarita do guarda. Esperei um pouco para que a telefonista não reconhecesse a minha voz. Depois de algum tempo liguei e disse: "Temos uma reclamação de que o telefone da guarita do guarda em Ridge Road apresenta problemas intermitentes - eles ainda estão com problemas?" Ela afirmou que não sabia, mas ia fazer a ligação para mim.

O segurança respondeu: "Portão de Ridge Road, aqui é Ryan." Eu comecei: "Olá, Ryan, aqui é o Ben. Você está tendo problemas com os seus telefones aí?" Ele é apenas um guarda de segurança com um salário baixo, mas acho que ele foi bem treinado porque disse imediatamente: "Ben de quê? Qual é o seu sobrenome?" Continuei como se não tivesse ouvido. "Alguém reportou um problema antes."

Eu o ouvi segurando o telefone longe do rosto e gritando: "Hei, Bruce, Roger, houve algum problema com este telefone?" Ele voltou: "Não, não sabemos de nenhum problema."

"Quantas linhas telefônicas vocês tem aí?"

Ele havia esquecido a história do meu sobrenome. "Duas", ele respondeu.

"Em qual você está agora?"

"3140".

Pronto! "E ambos estão funcionando bem?"

"Parece que sim."

"Muito bem", eu salientei. "Ouça, Tom, se você tiver algum problema, basta nos ligar na empresa de telefonia a qualquer momento. Estamos aqui para ajudar."

O meu amigo e eu resolvemos visitar a fábrica na noite seguinte. No final daquela tarde liguei para a guarita do guarda usando o nome do funcionário de Marketing e disse: "Oi, aqui é Tom Stilton, de Gráficos. Estamos com um prazo vencendo aqui e dois rapazes estão chegando à cidade para ajudar. Provavelmente eles chegarão depois da uma ou das duas da manhã. Você ainda vai estar por aqui?"

Ele ficou satisfeito em dizer que não, ele saía à meia-noite.

Eu retruquei; "Bem, deixe um recado para o segurança do próximo turno. OK? Quando os dois rapazes aparecerem e disserem que vieram ver o Tom Stilton, é para deixá-los entrar — tudo bem?"

Sim, ele disse, estava tudo bem. Ele tomou nota do meu nome, do departamento e do número do ramal e disse que tomaria conta do assunto.

Chegamos ao portão um pouco depois das duas, dei o nome de Tom Stilton e um guarda sonolento apontou para a porta pela qual deveríamos entrar e onde deveríamos estacionar o carro.

Quando ele entrou no prédio, havia outra guarita de segurança na recepção, com o conhecido livro para as assinaturas dos funcionários que entravam após o expediente. Expliquei ao guarda que tinha um relatório que precisava estar pronto pela manhã e que esse meu amigo queria ver a fábrica. "Ele é louco por helicópteros", eu contei. "Acho que ele quer aprender a pilotar um." Ele pediu o meu crachá. Procurei em um bolso e depois nos outros e disse que devia ter deixado o crachá no carro. "Eu vou lá pegar", eu disse. "Isso só vai levar uns dez minutos." Ele afirmou: "Tudo bem, basta assinar o livro."

Caminhar por aquela linha de produção era muito emocionante. Até aquela jamanta do Leroy nos parar.

No escritório da segurança, imaginei que alguém de fora ficaria nervoso e assustado. Quando as coisas ficam feias, começo a dar a impressão de que estou realmente à vontade, como se eu fosse realmente quem digo ser e que é aborrecedor o fato de eles não acreditarem em mim.

Quando eles começaram a conversar para saber se deveriam ligar para a senhora que eu disse ser a minha chefe e foram procurar o número do seu telefone no computador, fiquei lá parado e pensando:

"Boa hora para parar com isso tudo". Mas havia o portão do estacionamento — mesmo que conseguíssemos sair do prédio, eles poderiam fechar o portão e nós nunca conseguiríamos.

Quando Leroy ligou para a senhora que era a chefe de Stilton e, em seguida, me passou o telefone, ela gritava: "Quem é, quem é você?" e eu continuava falando como se estivéssemos em meio a um bate-papo e depois desliguei.

Quanto tempo é preciso para encontrar alguém que pode dar um número de telefone de uma empresa no meio da noite? Achei que tinha menos de quinze minutos para sair de lá antes que a senhora ligasse para o escritório da segurança.

Saímos de lá o mais rápido que pudemos sem parecer que estávamos com pressa. Fiquei aliviado quando o segurança do portão nos deixou sair.

Analisando a trapaça

Vale a pena notar que no incidente real no qual esta história se baseia, os invasores são realmente adolescentes. A invasão foi feita por farra, só para ver se conseguiam fazer isso. Mas se foi tão fácil para uma dupla de adolescentes, teria sido mais fácil ainda para ladrões adultos, espiões industriais ou terroristas.

Como três seguranças experientes permitem que dois intrusos simplesmente saiam? E eles não eram quaisquer intrusos, mas sim uma dupla tão jovem que qualquer pessoa razoável suspeitaria.

Leroy ficou desconfiado a princípio. Ele estava certo em levá-los para o Escritório da Segurança, em questionar o rapaz que chamou a si mesmo de Tom Stilton e em verificar os nomes e os números de telefone que ele deu. Ele agiu corretamente ao fazer a ligação telefônica para o supervisor.

Mas, no final, foi enganado pelo ar de confiança e indignação do jovem. Esse não era o comportamento que ele esperaria de um ladrão ou de um intruso — apenas um empregado real teria agido daquela maneira... ou pelo menos foi isso o que supôs. Leroy deveria ter sido treinado para contar com uma identificação sólida e não com percepções.

Por que Leroy não desconfiou mais quando o jovem desligou o telefone sem passá-lo novamente para que ele ouvisse a confirmação diretamente de Judy Underwood e recebesse a sua garantia de que o garoto tinha um motivo para estar na fábrica àquela hora da noite?

Leroy foi enganado por um truque tão audacioso que deveria ser óbvio. Mas pense um instante sob o seu ponto de vista: uma pessoa com apenas o colégio, preocupado com o seu emprego, sem saber se deveria incomodar um gerente da empresa pela segunda vez no meio da noite. Se você estivesse no lugar dele, teria feito a ligação de confirmação?

Obviamente, uma segunda ligação não era a única ação possível. O que mais o segurança poderia ter feito?

Mesmo antes de fazer a ligação, ele poderia ter pedido à dupla para mostrar algum tipo de foto de identificação. Eles dirigiram até a fábrica e, assim, pelo menos um deles deveria ter uma carteira de motorista. O fato de eles terem dado originalmente nomes falsos ficaria óbvio (um profissional viria com um ID falso, mas esses adolescentes não tomaram esse cuidado). Em todo caso, Leroy deveria ter examinado as suas credenciais de identificação e deveria ter anotado as informações. Se ambos insistissem que não tinham identificação, ele os levaria até o carro para pegar o crachá que "Tom Stilton" dizia ter deixado lá.

Depois da ligação telefônica, um dos seguranças deveria ter permanecido com a dupla até que ela saísse do prédio. E, em seguida, deveria levá-los até o carro e anotado o número das placas. Se ele

fosse suficientemente observador, poderia ter notado que a placa (aquela que o atacante havia comprado em um ferro-velho) não tinha um selo válido de registro — e isso seria motivo suficiente para deter a dupla para mais investigações.

Recado do Mitnick

As pessoas manipuladoras em geral têm personalidades multo atraentes, Elas geralmente são rápidas e bem articuladas. Os engenheiros sociais também são habilidosos para distrair os processos de pensamento das pessoas para que elas cooperem. Pensar que determinada pessoa não é vulnerável a essa manipulação é subestimar a habilidade e o instinto mortal do engenheiro social. Um bom engenheiro social, por sua vez. nunca subestima o seu adversário.

VIRANDO LATAS

Virar latas é uma expressão que descreve colocar as mãos no lixo do alvo em busca de informações valiosas. A quantidade de informações que você pode ter sobre um alvo é impressionante.

A maioria das pessoas não dá atenção para aquilo que estão descartando em casa: contas de telefone, faturas de cartões de crédito, vidros com receitas médicas, extratos de banco, material relacionado com o trabalho e tantas outras coisas.

No trabalho, os empregados devem ter consciência de que as pessoas olham no lixo para obter informações com as quais elas possam se beneficiar.

Durante meus anos no colégio, eu costumava vasculhar a lata de lixo que ficava atrás dos prédios da empresa de telefonia — quase sempre sozinho, às vezes com amigos que compartilhavam do interesse de saber mais sobre a empresa de telefonia. Depois que se torna um "vira-lata" experiente, você aprende alguns truques. tais como os esforços especiais para evitar os sacos de lixo dos banheiros e a necessidade de usar luvas.

Virar latas não é algo agradável, mas a recompensa era extraordinária — listas telefônicas internas de empresas, manuais de computadores, listas de empregados, material impresso descartado mostrando como programar o equipamento da central telefônica e muito mais tudo lá a sua disposição.

Programava as visitas para as noites em que eram emitidos manuais, porque os contêineres de lixo tinham muitos manuais antigos, os quais foram descuidadamente jogados fora. E também fazia essas visitas em outras épocas, procurando memorandos, cartas, relatórios e assim por diante, os quais possam oferecer algumas gemas preciosas da informação.

Jargão

VIRAR LATAS **Vasculhar o lixo de uma empresa (quase sempre em um lixo externo e vulnerável) para encontrar informações descartadas que tivessem valor ou que fornecessem uma ferramenta a ser usada em um ataque da engenharia social, tal como os números de telefones internos ou os cargos.**

Ao chegar, encontrava algumas caixas de papelão; tirava-as e as colocava de lado. Se alguém me desafiasse, o que acontecia de vez em quando, dizia que um amigo meu estava se mudando e eu estava procurando caixas para ajudá-lo a embalar as coisas. O guarda nunca observou todos os documentos que eu havia colocado dentro das caixas para levar para casa. Em alguns casos, ele me dizia para ir embora e, assim, simplesmente ia para o escritório central de outra empresa de telefonia.

Não sei como isso funciona hoje, mas naqueles dias era fácil saber quais sacos poderiam conter algo interessante. O lixo que era varrido do chão e o lixo da lanchonete ficava solto nos sacos grandes, enquanto as cestas de lixo dos escritórios estavam todas alinhadas com sacos de lixo descartáveis brancos, os quais eram amarrados um a um pelo pessoal da limpeza.

Certa vez, enquanto pesquisava com alguns amigos, encontrei algumas folhas de papel rasgadas à mão, E não apenas rasgadas: alguém havia tido o trabalho de cortar as folhas em pedaços pequenos, iodos convenientemente jogados em um único saco de lixo de 20 litros. Levamos o saco para uma loja local de rosquinhas, jogamos os pedaços em uma mesa e começamos a montar folha por folha.

Todos gostávamos de montar quebra-cabeças, de modo que isso oferecia o estimulante desafio de um quebra-cabeça gigante... mas ele tinha mais do que uma recompensa infantil. Quando terminamos, tínhamos juntado toda a lista de nomes de contas e senhas de um dos sistemas de computador crítico para a empresa.

As nossas explorações de "vira-latas" valeram o risco e o esforço? Pode apostar que sim. Valeu mais ainda do que você imagina porque o risco é zero. Isso era verdadeiro naquela época e ainda é verdadeiro hoje. Desde que você não invada nenhuma propriedade, mexer no lixo de outra pessoa é algo 100% legal.

Obviamente, os phreakers e hackers não são os únicos que enfiam suas cabeças nas latas de lixo. Os departamentos de polícia de todo o país fazem isso regularmente, e de mafiosos a criadores de bichinhos de estimação já foram condenados com base em parte na evidência coletada de seus lixos. As agências de inteligência, incluindo a nossa própria, recorrem a esse método há anos.

Essa pode ser uma tática muito baixa para James Bond — os fãs do cinema podem preferir observá-lo perseguindo o vilão e levando uma beldade para a cama do que ficar de joelhos em algum lixo. Os espiões da vida real são menos enjoados quando algo de valor pode estar embalado entre cascas de banana e pó de café usado, entre jornais e listas de compras. Particularmente quando a coleta das informações não os coloca em risco.

O lixo que vale dinheiro

As corporações também jogam o jogo do "vira-lata". Os jornais tiveram um dia diferente em junho de 2000 ao reportar que a Oracle Corporation (cujo CEO, Larray Ellison, provavelmente seja o mais famoso inimigo da Microsoft) havia contratado uma empresa de investigação que havia sido pega com as mãos na botija. Parece que os investigadores queriam o lixo de uma localização de lobby suportada pela Microsoft, a ACT, mas não queriam se arriscar a serem pegos. De acordo com as noticias da imprensa, a empresa de investigações enviou uma mulher que ofereceu aos zeladores US$ 60 para deixar que ela pegasse o lixo da ACT. Eles recusaram. Ela voltou na noite seguinte, subiu a oferta para US$ 500 para os faxineiros e US$ 200 para os supervisores.

Os zeladores recusaram e a entregaram.

O conhecido jornalista on-line Declan McCullah, inspirando-se na literatura, chamou o seu artigo sobre o episódio no *Wired News* de "Foi a Oracle que espiou a MS". A revista *Time,* desmascarando Ellison, da Oracle, chamou seu artigo simplesmente de "Larry, o curioso".

Analisando a trapaça

Com base em minha própria experiência e na experiência da Oracle, você poderia se perguntar por que uma pessoa se importaria em correr o risco de roubar o lixo de outra.

A resposta, acho, é que o risco é nulo e os benefícios podem ser substanciais. Muito bem, talvez tentar subornar os zeladores seja algo que aumente a chance de haver conseqüências, mas para aqueles que estão dispostos a se sujar um pouco, os subornos não são necessários.

Para um engenheiro social, a prática de virar latas tem seus benefícios. Ele pode obter informações suficientes para orientar o seu assalto contra a empresa-alvo, incluindo memorandos, agendas de reuniões, cartas e outros documentos que revelam nomes, departamentos, cargos, números de telefone e designações de projetos. O lixo pode render gráficos da organização, informações sobre a estrutura corporativa, cronogramas de viagens e outros. Todos esses detalhes podem parecer triviais para quem está dentro, embora sejam informações valiosíssimas para um atacante.

Mark Joseph Edwards, em seu livro *Internet Security with Windows* AT, fala sobre "relatórios inteiros descartados por causa de erros de digitação, senhas escritas em pedaços de papel, impressos de recados com números de telefone, pastas de arquivo inteiras com os documentos ainda dentro delas, disquetes e fitas que não foram apagados ou destruídos — tudo o que poderia ajudar um provável intruso".

O escritor pergunta: "E quem são as pessoas que trabalham na sua equipe de limpeza? Você decidiu que eles não entrarão [terão autorização] na sala dos computadores, mas não se esqueça das outras latas de lixo. Se as agências federais acharem necessário fazer verificações do histórico das pessoas que têm acesso às suas cestas de lixo e cortadores de papel, você provavelmente deve achar também."

Recado do Mitnick

O seu lixo pode ser o tesouro do seu inimigo. Não damos muita atenção para os materiais que descartamos em nossa vida pessoal e, assim, por que acreditaríamos que as pessoas têm uma atitude diferente no local de trabalho? Tudo se resume a educar a força de trabalho sobre o perigo (as pessoas inescrupulosas que vasculham informações valiosas) e a vulnerabilidade (as informações confidenciais que não estão sendo destruídas ou apagadas adequadamente).

O CHEFE HUMILHADO

Ninguém pensou em nada disso quando Harlan Fortis veio trabalhar na segunda-feira de manhã como sempre no Departamento Local de Trânsito e disse que ele saiu correndo de casa e esqueceu o crachá. O guarda da segurança vira Harlan chegando e saindo todos os dias úteis durante os dois anos nos quais ela vinha trabalhando naquele lugar. Ele fez um crachá temporário de empregado, ele pegou o crachá e continuou seu caminho.

Dois dias depois o inferno todo começou a acontecer. A história se espalhou por todo o departamento como um incêndio na floresta. Metade das pessoas que ouviram o que aconteceu não acreditou. Do restante, ninguém parecia saber se ria ou se chorava pela pobre alma.

Afinal de contas, George Adamson era uma pessoa gentil e generosa, a melhor cabeça que já haviam tido naquele departamento. Ele não merecia o que acontecera com ele. Tudo isso supondo que a história fosse verdadeira, é claro.

O problema havia começado quando George ligou para Harlan no seu escritório no final de uma sexta-feira e disse, com o máximo possível de gentileza, que a partir da segunda-feira Harlan teria um novo emprego no Departamento Sanitário. Para Harlan isso não era como ser despedido, isso era pior, pois era humilhante. Ele não ia deixar isso barato.

Naquela mesma noite ele sentou-se na varanda para observar o trânsito das pessoas que voltavam para casa. Finalmente encontrou um garoto da vizinhança chamado David, o qual era chamado por iodos de "O garoto dos jogos de guerra", voltando para casa, vindo do colégio. Ele parou David, deu-lhe um *"Code Red Mountain Dew"* que havia comprado especialmente com essa finalidade e fez a proposta: o *videogame* mais recente e seis jogos em troca de ajuda com o computador e a promessa de ficar com o bico calado.

Depois que Harlan explicou o projeto — sem dar nenhum detalhe comprometedor —, David concordou. Ele descreveu o que queria que Harlan fizesse. Ele teria de comprar um modem, ir até o escritório, encontrar o computador de alguém no qual houvesse um conector de telefone perto e desocupado e ligar o modem. Teria de deixar o modem sob a mesa, em um lugar onde ninguém poderia ver. Em seguida, viria a parte arriscada. Harlan tinha de se sentar ao computador, instalar um software de acesso remoto e fazê-lo funcionar sempre que o homem que trabalhava no escritório aparecia, ou sempre que alguém entrava e o via no escritório de outra pessoa. Ele estava tão tenso que mal podia ler as instruções que o garoto havia escrito para ele. Mas ele conseguiu e saiu do prédio sem ser visto.

Plantando a bomba

Naquela noite David veio após o jantar. Os dois se sentaram no computador de Harlan e em alguns minutos o garoto havia discado para o modem, ganhado acesso e chegado à máquina de George Adamson. Isso não foi muito difícil, uma vez que George nunca teve tempo para medidas de segurança, tais como mudar as senhas, e estava sempre pedindo para uma ou outra pessoa fazer o download ou o envio por e-mail de algum arquivo para ele. Em pouco tempo, todos que trabalhavam no escritório sabiam qual era a sua senha.

Um pouco de pesquisa revelou o local onde estava o arquivo chamado BudgetSlides2002.ppt e o garoto fez o download dele no computador de Harlan. Em seguida, Harlan disse ao garoto para ir para casa e voltar em duas horas.

Quando David voltou, Harlan pediu para ele se reconectar ao sistema de computadores do Departamento de Estradas *e* colocar o mesmo arquivo de volta no lugar onde o encontrara para sobregravar a versão anterior. Harlan mostrou a David o *videogame* e prometeu que se as coisas corressem bem, ele o teria no dia seguinte.

Surpreendendo George

Você não imagina que algo tão sem graça quanto audiências de orçamento teriam interesse para alguém, mas a sala de reuniões do Conselho Local estava cheia de repórteres, representantes de grupos de interesses especiais, membros do público e até mesmo duas novas equipes de televisão.

George sempre achou que havia muita coisa em jogo nessas sessões. O Conselho Local tinha as rédeas da situação e, a menos que George pudesse fazer uma apresentação convincente, o orçamento de Estradas seria cortado. Em seguida, alguém começaria a reclamar sobre buracos, semáforos quebrados e cruzamentos perigosos, o culparia e a vida ficaria terrível no ano seguinte. Mas quando

foi apresentado naquela noite, ele se levantou confiante. Ele havia trabalhado seis semanas nessa apresentação e nos slides do PowerPoint. Ele havia testado com a sua mulher, com as principais pessoas da sua equipe e com alguns amigos respeitados. Todos concordaram que essa era a melhor apresentação que já haviam visto.

As três primeiras imagens do PowerPoint ficaram boas. Para variar, todos os membros do Conselho estavam prestando atenção. Ele estava passando as suas idéias de modo eficaz.

De repente tudo começou a sair errado. A quarta imagem deveria ser uma linda foto ao pôr-do-sol da nova extensão da rodovia que havia sido inaugurada no ano passado. Em vez disso, algo muito embaraçoso aconteceu. A foto era de uma revista do tipo *Penthouse* ou *Hustler*. O público estava boquiaberto e ele correu até o laptop para mudar para a próxima imagem.

Essa era pior ainda. Não havia nada a ser imaginado.

Ele ainda estava tentando clicar em outra imagem quando alguém do público desligou o cabo de força do projetor enquanto o diretor batia ruidosamente o seu martelo e gritava mais alto do que o barulho do público dizendo que a reunião eslava adiada.

Analisando a trapaça

Usando a experiência de um hacker adolescente, um empregado desgostoso conseguiu acessar o computador do chefe do seu departamento, descarregar uma importante apresentação do PowerPoint e substituir alguns dos slides por imagens que certamente causariam um embaraço sério. Em seguida, ele colocou a apresentação de volta no computador do homem.

Com o modem conectado a um dos computadores do escritório, o jovem hacker conseguia discar de fora. O garoto havia configurado o software de acesso remoto com antecedência para que, após estar conectado ao computador, ele tivesse acesso completo a cada arquivo que estivesse armazenado em todo o sistema. Como o computador estava conectado à rede da organização e já tinha o nome e a senha do chefe, ele pode facilmente acessar os arquivos do chefe.

Incluindo o tempo para escanear as imagens das revistas, todo o esforço havia levado apenas quatro horas. O dano resultante para a reputação de um bom homem ia além do que se possa imaginar.

Recado do Mitnick

A grande maioria dos empregados que são transferidos, demitidos ou rebaixados nunca causa problemas. Mesmo assim é preciso apenas um deles para fazer uma empresa perceber tarde demais as medidas que poderiam ser tomadas para evitar o desastre. A experiência e as estatísticas têm mostrado claramente que a maior ameaça para a empresa vem de *dentro.* São as pessoas que estão dentro que têm um conhecimento grande do lugar onde ficam as informações valiosas e de onde a empresa pode ser atingida para causar o maior dano.

O CAÇA-PROMOÇÕES

No final da manhã de um agradável dia de outono, Peter Milton caminhava na recepção dos escritórios regionais em Denver da Honorable Auto Parts, um atacadista nacional de peças para o mercado de automóveis. Ele aguardava na recepção enquanto a jovem registrava um visitante, dava orienta-

çôes para uma pessoa ao telefone sobre como chegar ao prédio e lidava com o homem do UPS, tudo mais ou menos ao mesmo tempo.

"Como você aprendeu a fazer tantas coisas ao mesmo tempo?", disse Pete quando ela teve tempo para ajudá-lo. Ela sorriu, obviamente satisfeita porque ele havia notado. Ele era do departamento de Marketing do escritório de Dallas, como contou a ela, e disse também que Mike Talbott das vendas regionais de Atlanta ia recebê-lo. "Temos um cliente para visitar esta tarde", ele explicou. "Vou aguardar aqui na recepção."

"Marketing". Ela disse a palavra pensativamente, e Peter sorriu para ela esperando o que viria a seguir. "Se eu pudesse fazer faculdade, é isso o que escolheria", afirmou ela. "Adoraria trabalhar em Marketing."

Ele sorriu novamente. "Kaila", ele continuou, lendo o nome na placa que estava no balcão, "Temos uma senhora no escritório em Dallas que foi secretária. Ela conseguiu ser transferida para o Marketing. Isso foi há três anos e agora ela é gerente assistente de marketing ganhando o dobro do que ganhava."

Kaila ficou estarrecida. Ele continuou: "Você sabe usar um computador?"

"E claro que sim", ela disse.

•Você gostaria que eu colocasse o seu nome para se inscrever para um cargo de secretária no Marketing?"

Ela ficou radiante. "Eu seria capaz até de me mudar para Dallas."

"Você vai adorar Dallas", ele disse. "Não posso prometer uma vaga imediatamente, mas vou ver o que posso fazer."

Ela pensou que aquele homem simpático, no seu terno e gravata e com os cabelos bem cortados e penteados, poderia fazer uma grande diferença para a sua vida profissional.

Pete sentou-se do outro lado da recepção, abriu o seu laptop e começou a trabalhar. Após dez ou quinze minutos, ele voltou ao balcão. "Ouça", ele retorquiu, "parece que Mike deve estar ocupado. Há uma sala de reuniões onde eu possa me sentar e verificar os meus e-mails enquanto espero?"

Kaila ligou para o homem que coordenava a programação das salas de reunião e conseguiu uma que não estava ocupada para Pete. Seguindo o padrão usado nas empresas do Vale do Silício (provavelmente a Apple foi a primeira a adotá-lo), algumas das salas de reuniões tinham nomes de personagens de desenhos animados, outras de cadeias de restaurantes, estrelas de cinema ou heróis de histórias em quadrinhos. Ele disse para procurar a sala Minnie. Ela o registrou e deu as orientações para ele encontrar a Minnie.

Ele localizou a sala, acomodou-se e conectou o seu laptop à porta Ethernet.

Você já adivinhou o que aconteceu?

Certo — o intruso havia se conectado à rede *atrás do firewall corporativo.*

A história de Anthony

Acho que podemos chamar Anthony Lake de um homem de negócios preguiçoso. Ou talvez "encostado" ficasse melhor.

Em vez de trabalhar para as outras pessoas, ele havia decidido que queria trabalhar para si mesmo. Queria abrir uma loja, na qual pudesse estar em um local o dia todo e não precisasse percorrer o país inteiro. Só que ele queria ter uma empresa na qual tivesse quase certeza de ganhar dinheiro.

Que tipo de loja? Não *é* preciso muito tempo para descobrir. Ele sabia consertar carros e, então, a opção lógica seria uma loja de autopeças.

E como você cria uma garantia de sucesso? A resposta veio num instante: convencer o atacadista de autopeças Honorable Auto Parts a vender-lhe toda a mercadoria de que precisava com o seu custo.

Naturalmente eles não fariam isso de livre e espontânea vontade. Mas Anthony sabia como enganar as pessoas, o seu amigo Mickey sabia como invadir os computadores das outras pessoas e juntos imaginaram um plano inteligente.

Naquele dia de outono ele passou por um empregado chamado Peter Milton e conseguiu entrar nos escritórios da Honorable Auto Paris e já havia conseguido ligar o seu laptop à rede da empresa. Até aqui. tudo bem, mas essa foi apenas a primeira etapa. Aquilo que ainda teria de fazer não seria fácil, particularmente porque Anthony havia definido um limite de 15 minutos para si mesmo — um pouco mais e ele calculava que o risco de ser descoberto seria muito alto.

Em uma ligação telefônica anterior, fingindo ser uma pessoa do suporte do fornecedor de computadores, ele havia dado outro golpe. "A sua empresa comprou um plano de suporte por dois anos e estamos colocando vocês no banco de dados para sabermos quando um programa de software que vocês usam terá um patch ou uma versão atualizada. Assim sendo, preciso que vocês me digam quais aplicativos vocês usam." A resposta deu-lhe uma lista de programas e um amigo contador identificou um chamado MAS 90 como o alvo — o programa que manteria a lista de fabricantes, juntamente com o desconto e os prazos de pagamento de cada um.

Recado do Mitnick

Treine o seu pessoal para não julgar um livro apenas pela capa — o fato de alguém estar bem vestido e bem penteado não faz dela uma pessoa mais confiável.

Com esse importante conhecimento, ele usou um programa de software para identificar todos os hosts em funcionamento na rede e não demorou muito para que localizasse o servidor correto usado pelo departamento Contábil Do arsenal de ferramentas de hacker do seu laptop, ele abriu um programa e o usou para identificar todos os usuários autorizados no servidor de destino. Com outro programa, executou uma lista das senhas mais usadas, tais como "branco" e a própria "senha". "Senha" funcionou e isso não foi surpresa. As pessoas perdem toda a criatividade na hora de escolher as senhas.

Apenas seis minutos depois o jogo já estava acabado e ele estava dentro da empresa.

Mais outros três minutos para incluir com todo o cuidado o nome da sua empresa, endereço. número de telefone e nome para contato na lista de clientes. E, em seguida, a entrada crucial, aquela que faria toda a diferença, a entrada que dizia todos os itens que lhe foram vendidos a 1% acima do custo da Honorable Auto Paris.

Em aproximadamente dez minutos ele havia terminado. Ele parou o tempo suficiente para agradecer a Kaila e dizer que já tinha verificado seus e-mails. E ele havia falado com Mike Talbot. os planos haviam mudado e ele estava indo para uma reunião no escritório do cliente. E ele não se esqueceria de recomendá-la para aquele trabalho em Marketing.

Analisando a trapaça

O intruso que chamou a si mesmo de Peter Milton usou duas técnicas de subversão psicológica — uma planejada e a outra improvisada com o desenrolar dos acontecimentos.

Ele se vestiu como um funcionário do gerenciamento que ganha um bom dinheiro. Terno e gravata, cabelo bem cuidado — esses parecem ser detalhes pequenos, mas eles causam uma boa impressão. Eu mesmo descobri isso sem querer. Em pouco tempo como programador da GTE Califórnia — uma grande empresa de telefonia que não existe mais — descobri que se viesse um dia sem o crachá, bem vestido, mas com roupa esporte — digamos uma camisa, calça e sapatos esporte — eu era parado e questionado. Onde está o seu crachá, quem é você, onde você trabalha? Outro dia eu chegava, ainda sem o crachá, mas com terno, gravata e aparência bem corporativa. Eu usava uma variação de uma velha técnica e me misturava a multidão de pessoas que entrava em um prédio ou portaria de segurança. Eu ficava perto de alguém ao passar pela entrada principal e caminhava conversando com as pessoas como se fosse uma delas. Eu passava e mesmo que os guardas notassem que eu estava sem crachá, eles não se importavam comigo porque eu tinha aparência de quem trabalhava na gerência e estava com as pessoas que *usavam* crachás.

Dessa experiência reconheci como o comportamento dos guardas de segurança era previsível. Assim como o restante de nós, eles faziam julgamentos com base em aparências — uma vulnerabilidade séria que os engenheiros sociais aprenderam a aproveitar.

A segunda arma psicológica do atacante entrou em ação quando ele observou o esforço incomum que a recepcionista estava fazendo. Fazendo várias coisas ao mesmo tempo, ela não se atrapalhou, mas conseguiu fazer com que todos se sentissem bem atendidos. Ele interpretou isso como um sinal de alguém que está interessado em avançar e melhorar. Em seguida, quando disse que trabalhava no departamento de Marketing, ele observou a sua reação, procurando pistas que indicassem que ele estava estabelecendo uma identificação com ela. E ele estava. Para o atacante isso se traduzia em alguém que poderia ser manipulado com uma promessa de tentar ajudá-la a conseguir um trabalho melhor (Obviamente, se ela quisesse trabalhar no departamento Contábil, ele diria que teria contatos e poderia conseguir um trabalho para ela naquele departamento.)

Os invasores também gostam de outra arma psicológica que é usada nesta história: a criação da confiança com um ataque em dois estágios. Primeiro ele usou aquela conversa sobre o trabalho em Marketing e também usou a técnica do "namedropping" — dar o nome de outro empregado —, uma pessoa real que, por acaso, tinha o mesmo nome que ele usou.

Recado do Mitnick

A permissão para que um estranho entre em uma área onde pode conectar um laptop na rede corporativa aumenta o risco de um incidente de segurança. É perfeitamente razoável deixar que um empregado, particularmente de outro escritório, verifique seus e-mails em uma sala de reuniões, mas a menos que o visitante seja estabelecido como alguém de confiança ou que a rede esteja segmentada para evitar conexões não autorizadas, esse pode ser o elo mais fraco que permite que os arquivos da empresa sejam comprometidos.

Ele poderia ter feito a solicitação de usar uma sala de reuniões imediatamente após a conversa inicial. Mas em vez disso preferiu se sentar por algum tempo e fingir estar trabalhando, supostamente

enquanto esperava o seu colega, outra forma de evitar qualquer suspeita possível porque um invasor não ficaria por ali. Ele não ficou muito tempo, porém; os engenheiros sociais sabem melhor do que ninguém que não devem ficar na cena do crime além do tempo necessário.

Pelas leis da época em que este livro foi escrito, Anthony não havia cometido um crime quando entrou na recepção. Não havia cometido um crime quando usou o nome de um empregado real. Não cometeu um crime quando conseguiu entrar na sala de reuniões. Não havia cometido um crime ao se ligar à rede da empresa e pesquisar o computador-alvo. Antes de realmente entrar no sistema de computadores, ele não havia infringido a lei.

BISBILHOTANDO KEVIN

Há muitos anos, quando trabalhava em uma empresa pequena, sempre que entrava no escritório que compartilhava com três outras pessoas que formavam o departamento de TI eu observava que esse rapaz em particular (aqui eu vou chamar de Joe) rapidamente mudava o monitor do seu computador para uma janela diferente. Imediatamente reconheci isso como um comportamento suspeito. Quando isso aconteceu duas ou mais vezes no mesmo dia. tive certeza de que algo estava acontecendo e eu deveria descobrir. O que esse rapaz estava fazendo e não queria que eu visse?

O computador de Joe agia como um terminal para acessar os minicomputadores da empresa, de modo que instalei um programa de monitoramento no minicomputador VAX que me permitia espiar o que ele estava fazendo. O programa agia como se uma câmera de TV espiasse sobre o seu ombro e me mostrasse exatamente aquilo que ele estava vendo no seu computador.

A minha mesa era próxima da do Joe; ajustei o meu monitor na melhor posição possível para que ele não o visse, mas ele poderia ter olhado a qualquer momento e percebido que eu o estava espiando. Isso não era problema, porque ele estava tão envolvido naquilo que estava fazendo que nem notaria.

O que vi fez o meu queixo cair. Eu observei, fascinado, o bandido chamar os dados da *minha* folha de pagamento. Ele estava olhando o meu salário!

Na época eu trabalhava lá há poucos meses e achei que Joe não suportava a idéia de que eu poderia estar ganhando mais do que ele.

Alguns minutos depois vi que ele estava fazendo o download de ferramentas de hacker que são usadas pelos hackers menos experientes, que não conhecem o suficiente de programação para criar as ferramentas para si mesmos. Assim sendo, Joe não tinha a menor idéia de que um dos hackers mais experientes da América estava sentado bem ao seu lado. Achei isso muito divertido.

Ele já tinha a informação sobre o meu salário; assim sendo, era tarde demais para tentar impedi-lo. Além disso, qualquer empregado que tenha acesso por computador à Receita Federal (1RS) ou à Administração do Seguro Social pode consultar o seu salário. Certamente eu não queria que ele soubesse que eu descobrira o que ele estava fazendo. O meu principal objetivo na época era ser discreto, e um bom engenheiro social não anuncia as suas habilidades e o seu conhecimento. Você sempre quer que as pessoas o subestimem e não que o vejam como uma ameaça.

Assim sendo, deixei tudo como estava e ri sozinho porque Joe achava que sabia algum segredo sobre mim, quando o que acontecia era exatamente o contrário: eu tinha a última palavra porque sabia o que ele estava fazendo.

Depois descobri que todos os meus três colegas do grupo de TI se divertiam olhando o salário desta ou daquela secretária bonitinha (no caso da única garota do grupo) ou daquele rapaz bonitão

que eles haviam descoberto. E todos estavam descobrindo o salário e os bônus de qualquer pessoa da empresa sobre quem estivessem curiosos, incluindo a gerência de primeiro escalão.

Analisando a trapaça

Esta história ilustra um problema interessante. Os arquivos da folha de pagamento podiam ser acessados pelas pessoas que tinham a responsabilidade de manter os sistemas de computadores da empresa. Assim sendo, tudo era uma questão pessoal: resolver em quem confiar. Em alguns casos, a equipe de TI poderia achar irresistível bisbilhotar um pouco. E eles tinham a capacidade de fazer isso porque tinham privilégios que lhes permitiam desviar dos controles de acesso daqueles arquivos.

Uma medida de segurança seria auditar todo acesso a arquivos confidenciais, tais como a folha de pagamento. Obviamente, todos que tinham os privilégios requisitados poderiam desativar a auditoria ou talvez remover todas as entradas que apontassem para eles, mas cada etapa adicional exigia mais esforço para ser ocultada por parte de um empregado inescrupuloso.

EVITANDO A TRAPAÇA

De virar a sua lata de lixo até enganar um guarda de segurança ou uma recepcionista, os engenheiros sociais podem invadir fisicamente o seu espaço corporativo. Mas você vai gostar de ouvir que há precauções que você pode tomar.

Proteção após o horário de expediente

Todos os empregados que chegam para trabalhar sem seus crachás devem parar na mesa da recepção ou no escritório da segurança para conseguir um crachá temporário a ser usado naquele dia. O incidente da primeira história deste capítulo poderia ter uma conclusão muito diferente se o guarda da empresa tivesse recebido um conjunto específico de etapas a serem seguidas quando encontrasse alguém sem o crachá de empregado requerido.

Nas empresas ou áreas dentro de uma empresa nas quais a segurança não é a principal preocupação, talvez não faça sentido insistir para que cada pessoa mantenha um crachá visível durante todo o tempo. Mas nas empresas que têm áreas confidenciais, esse deve ser um requisito-padrão, o qual deve ser implantado com rigidez. Os empregados devem ser treinados e motivados a desafiar as pessoas que não têm um crachá, e os empregados de nível mais alto devem ser ensinados a aceitar esses desafios sem causar nenhum embaraço para as pessoas que os pararem.

A política da empresa deve avisar os empregados sobre as penalidades para aqueles que não usam seus crachás; as penalidades podem incluir o envio do empregado para casa naquele dia sem direito ao pagamento ou uma anotação no seu arquivo pessoal. Algumas empresas instituem uma série de penalidades progressivamente mais rígidas que podem incluir o relato do problema para o gerente da pessoa e, em seguida, a emissão de um aviso formal.

Além disso, quando houver informações confidenciais a serem protegidas, a empresa deve estabelecer procedimentos para autorizar as pessoas que precisam estar na empresa fora do expediente. Uma solução seria exigir que fossem tomadas providências por parte da segurança corporativa ou de algum outro grupo designado. Esse grupo verificaria rotineiramente a identidade de todos os empregados que ligassem pedindo uma visita fora do expediente por meio de uma ligação para o supervisor daquela pessoa ou usando algum outro meio relativamente seguro.

Tratando o lixo com respeito

A história do "vira-latas" falou do mau uso do seu lixo corporativo. Os oito segredos para tratar o lixo com sabedoria são:

- Classificar todas as informações confidenciais com base no grau de confidencialidade.
- Estabelecer procedimentos em toda a empresa para descartar as informações confidenciais.
- Insistir em que todas as informações confidenciais descartadas passem primeiro pela máquina cortadora de papel e fornecer um modo seguro de se livrar das informações importantes em pedaços de papel que são pequenos demais e passam pela máquina. As máquinas não devem ser muito baratas, as quais resultam em tiras de papel que podem ser montadas novamente por um atacante determinado e com paciência. Elas devem ser do tipo que faz cortes cruzados ou do tipo que transforma a saída em polpa inútil.
- Fornecer um modo de inutilizar ou apagar *completamente* a mídia de computador — os disquetes, discos Zip, CDs e DVDs usados para armazenar arquivos, fitas removíveis ou unidades de disco rígido antigas e outras mídias de computador — antes de descartá-la. Lembre-se de que os arquivos apagados *não* são realmente removidos; eles ainda podem ser recuperados — como descobriram os executivos da Enron e muitos outros. Jogar simplesmente a mídia de computador no lixo é um convite para o seu "vira-latas" local de plantão. (Consulte o Capítulo 16 para obter as orientações específicas sobre como eliminar mídia e dispositivos.)
- Manter um nível de controle apropriado sobre a seleção das pessoas da sua equipe de limpeza usando a verificação de antecedentes, se for apropriado.
- Fazer com que os empregados pensem periodicamente na natureza do material que estão jogando no lixo.
- Trancar os contêineres de lixo.
- Usar contêineres separados para material confidenciai e fazer com que os materiais dispensados sejam manuseados por uma empresa especializada nesse trabalho.

Dizendo adeus aos empregados

Anteriormente nós destacamos a necessidade de procedimentos rígidos quando o empregado de um departamento tiver acesso a informações confidenciais, senhas, números de discagem e outros. Os seus procedimentos de segurança precisam fornecer um modo de controlar as pessoas que têm autorização de acesso a vários sistemas. Pode ser difícil evitar que determinado engenheiro social burle as barreiras da sua segurança, mas não facilite isso para um ex-empregado.

Outra etapa que é ignorada. Quando um empregado que tinha autorização de recuperação de fitas de backup em uma empresa de armazenamento vai embora, uma política por escrito deve pedir que a empresa de armazenamento seja notificada imediatamente para remover o seu nome da lista de pessoas autorizadas.

O Capítulo 16 deste livro fornece informações detalhadas sobre esse assunto vital, mas é útil relacionar aqui algumas das principais medidas de segurança que devem ser usadas, como deixou claro esta história:

- Um checklist completo das etapas a serem tomadas quando um empregado vai embora, com providências especiais para os funcionários que tinham acesso a dados confidenciais.

- Uma política de encerramento *imediato* do acesso do empregado ao computador — de preferência antes de a pessoa deixar o prédio.
- Um procedimento para recuperar o crachá de identificação da pessoa, bem como de todas as chaves ou dispositivos de acesso eletrônico.
- Medidas que exijam que os guardas da segurança vejam o ID com foto antes de admitir qualquer empregado que não tenha o seu passe de segurança, e a verificação do nome em uma lista para saber se a pessoa ainda é funcionária da organização.

Algumas outras etapas parecerão excessivas ou caras demais para algumas empresas, mas elas são apropriadas para outras. Essas medidas de segurança mais rígidas incluem:

- Crachás de identificação eletrônica combinados com scanners nas entradas; cada empregado passa o seu crachá no scanner para a determinação eletrônica instantânea de que a pessoa ainda é um empregado e pode entrar no prédio. (Observe, porém, que os guardas da segurança precisam estar alertas para a tática na qual uma pessoa não autorizada entra junto com um empregado legítimo.)
- Uma ordem para que todos os empregados do mesmo grupo da pessoa que está saindo (particularmente se a pessoa está sendo demitida) mudem suas senhas. (Isso parece extremo? Muitos anos após o curto período de tempo em que estive na General Telephone, soube que o pessoal da segurança da Pacific Bell, ao ouvir falar que a General Telephone havia me contratado, "morreu de rir". Mas para crédito da General Telephone, quando perceberam que tiveram um hacker conhecido trabalhando para eles, e após me demitirem, pediram que as senhas de *todos que trabalhavam na empresa* fossem trocadas!).

Você não quer que as suas instalações se pareçam com cadeias, mas ao mesmo tempo precisa se defender contra o funcionário que foi demitido ontem, mas que hoje volta com intenção de causar danos.

Não se esqueça de ninguém

As políticas de segurança tendem a ignorar o empregado do nível iniciante, aquelas pessoas como as recepcionistas, que não lidam com informações corporativas confidenciais. Já vimos que as recepcionistas são um alvo útil para os atacantes, e a história da invasão da empresa de autopeças fornece outro exemplo: uma pessoa amistosa, vestida com um profissional que alega ser um empregado de outro escritório da organização pode não ser o que parece. As recepcionistas precisam ser bem treinadas sobre como pedir educadamente o ID da empresa quando for apropriado, e o treinamento precisa incluir não apenas a recepcionista principal, mas também todos os que se sentam na recepção para descansar no horário de almoço ou nos intervalos.

Para os visitantes de fora da empresa, a política deve exigir que um ID com foto seja mostrado e as informações sejam registradas. Não é difícil obter um ID falso, mas pelo menos a exigência de um ID complica um pouco mais as coisas para um pretenso atacante.

Em algumas empresas é lógico seguir uma política que requer que os visitantes sejam acompanhados da recepção e de uma sala de reunião para outra. Os procedimentos devem exigir que o acompanhante deixe claro quando entregar o visitante no seu primeiro compromisso que essa pessoa entrou no prédio como empregado ou não empregado. Por que isso é importante? Porque como vimos nas histórias anteriores, um atacante quase sempre se faz passar por alguém para a primeira pessoa

que ele encontrou e por outro alguém para a próxima pessoa que encontra. E fácil para um atacante aparecer na recepção, convencer a recepcionista de que tem um compromisso com um engenheiro, por exemplo, e depois ser acompanhado até o escritório do engenheiro, onde diz ser um representante de uma empresa que quer vender algum produto para a empresa e, então, após a reunião com o engenheiro, ele tem acesso livre para perambular pelo prédio.

Antes de admitir um empregado de outro escritório nas instalações da empresa, devem ser seguidos procedimentos adequados para verificar se a pessoa é verdadeiramente um empregado. As recepcionistas e os seguranças devem conhecer os métodos usados pelos atacantes para usar a identidade de um empregado e ter acesso aos prédios da empresa.

Como se proteger contra o atacante que consegue entrar dentro do prédio e ligar o seu laptop em uma porta de rede atrás do firewall corporativo? Dada a tecnologia atual, isso é um desafio: salas de reunião, salas de treinamento e áreas similares não devem deixar as portas de rede sem segurança, mas devem protegê-las com firewalls ou roteadores. Entretanto, a melhor proteção vem do uso de um método seguro de autenticar todos os usuários que se conectam à rede.

TI segura!

Um conselho: na sua própria empresa, cada funcionário de TI provavelmente sabe ou pode descobrir em momentos quanto você está ganhando, quanto o CEO recebe e quem está usando o jatinho corporativo para ir esquiar nas férias.

Em algumas empresas é até mesmo possível que o pessoal de TI ou o pessoal da contabilidade aumente os próprios salários, faça pagamentos para um fornecedor falso, remova as classificações negativas dos registros do RH e assim por diante. As vezes, apenas o medo de ser pego os mantêm honestos... e chega um dia em que alguém cujo ódio ou desonestidade natos faz com que ele ignore o risco e faça tudo que acha que pode fazer.

E claro que existem soluções. Os arquivos confidenciais podem ser protegidos com controles de acesso adequados para que apenas o pessoal autorizado possa abri-los. Alguns sistemas operacionais têm controles de auditoria que podem ser configurados para manter um registro de determinados eventos, tais como cada pessoa que tenta acessar um arquivo protegido, independentemente da tentativa ter ou não sucesso.

Se a sua empresa entendeu essa questão e implementou controles de acesso adequados e auditorias que protegem os arquivos confidenciais, então você está tomando medidas poderosas na direção certa.

Capítulo 11

Combinando a Tecnologia e a Engenharia Social

Um engenheiro social vive da sua capacidade de manipular as pessoas para que elas façam coisas que o ajudem a atingir o seu objetivo, mas o sucesso quase sempre requer uma grande dose de conhecimento e habilidade com os sistemas de computador e telefonia.

Esta é uma amostragem dos golpes da engenharia social nos quais a tecnologia teve um papel importante.

O HACKING ATRÁS DAS GRADES

Quais são algumas das instalações mais seguras que você consegue imaginar, protegidas contra invasões, sejam elas de natureza física, de telecomunicações ou eletrônicas? Fort Knox? Não. A Casa Branca? Também não. NORAD, a instalação da defesa norte-americana enterrada nas profundezas de uma montanha? Certamente que não.

E as prisões e os centros de detenção federais? Eles devem ser tão seguros quanto qualquer outro lugar do país, certo? As pessoas raramente escapam, e quando conseguem, normalmente são presas logo. Você deve achar que uma instalação federal não está vulnerável aos ataques da engenharia social. Mas está errado — não existe segurança à toda a prova em lugar algum.

Há alguns anos, uma dupla de grifters (trapaceiros profissionais) estava com um problema. Acontece que eles haviam roubado uma grande soma em dinheiro de um juiz local. A dupla já era procurada pela lei há muito tempo, mas desta vez as autoridades federais se interessaram pelo caso. Elas pegaram um dos grifters. Charles Gondorff, e o colocaram em um centro correcional perto de São Diego. O magistrado federal ordenou que ele fosse detido como um criminoso frio e um perigo para a comunidade.

O seu colega Johnny Hooker sabia que Charlie ia precisar de um bom advogado de defesa. Mas de onde viria o dinheiro para pagá-lo? Assim como a maioria dos grifters, o seu dinheiro sempre havia sido gasto em roupas boas, carros novos e mulheres assim que era ganho. Johnny raramente tinha o suficiente para viver.

O dinheiro para pagar um bom advogado teria de vir de outro golpe. Johnny não podia fazer isso por conta própria. Charlie Gondorff sempre havia sido o cérebro de seus golpes. Mas Johnny não se atrevia a visitar o centro de detenção para perguntar a Charlie o que deveria fazer, não agora que os federais sabiam que havia dois homens envolvidos no golpe e estavam loucos para pegar o outro. Da mesma forma, apenas a família podia visitá-lo, e isso significava que ele teria de mostrar uma iden-

tificação falsa e dizer ser um membro da família. Tentar usar um ID falso em uma prisão federal não parecia ser uma idéia muito inteligente.

Não, ele teria de entrar em contato com Gondorff de outra maneira. Isso não seria fácil. Nenhum recluso de qualquer prisão federal, estadual ou municipal pode receber ligações telefônicas. Uma placa colocada ao lado de cada telefone de um centro de detenção federal diz algo do tipo "Todas as conversações feitas neste telefone estão sujeitas a monitoramento e o uso do telefone é considerado consentimento com o monitoramento". Ter os oficiais do governo ouvindo as suas ligações telefônicas enquanto se comete um crime é um modo de aumentar os seus planos de férias financiados pelo governo federal.

Johnny sabia, porém, que determinadas ligações telefônicas não eram monitoradas: as ligações entre um prisioneiro e seu advogado, as quais são protegidas pela Constituição como comunicações entre cliente e advogado, por exemplo. Na verdade, a prisão onde estava Gondorff tinha os telefones conectados diretamente ao Escritório do Defensor Público. Escolha um daqueles telefones e uma conexão direta é estabelecida com o telefone correspondente do EDP. A empresa de telefonia chama isso de *Conexão Direta.* As autoridades desavisadas supõem que o serviço é seguro e invulnerável porque as ligações feitas só podem ir para a Defensoria Pública, e as ligações recebidas são bloqueadas. Mesmo que alguém pudesse de alguma maneira encontrar o número do telefone, eles estariam programados na empresa de telefonia para *negar encerramento,* o qual é uma expressão complicada da empresa de telefonia para descrever o serviço no qual as ligações recebidas não são permitidas.

Como todo grifter meio decente conhece bem a arte da fraude, Johnny descobriu que tinha de haver um modo de contornar esse problema. Lá dentro Gondorff já havia tentado pegar um dos telefones do EDP e dizer: "Aqui é Tom, do centro de reparos da empresa de telefonia. Estamos executando um teste nessa linha e preciso que você tente discar nove, zero e zero." O nove acessaria uma linha externa, o zero, zero ligaria para uma telefonista de interurbano. Isso não funcionou — a pessoa que atendeu ao telefone no EDP já conhecia esse truque.

Johnny estava com mais sorte. Ele descobriu rapidamente que havia dez unidades no centro de detenção, cada uma com uma linha telefônica direta para o Escritório do Defensor Público. Johnny encontrou alguns obstáculos, mas como um bom engenheiro social que era, ele pôde pensar em modos de contornar esses empecilhos aborrecedores. Em qual unidade estava Gondorff? Qual era o número de telefone dos serviços de conexão direta daquela unidade? E como poderia mandar um recado inicial para Gondorff sem que ele fosse interceptado pelos agentes penitenciários?

O que parece ser impossível para a maioria das pessoas, como obter os números secretos dos telefones localizados nas instituições federais, quase sempre está a algumas ligações telefônicas de um verdadeiro golpista. Após algumas noites sem dormir criando um plano, Johnny acordou uma manhã com todo o plano traçado em sua mente. Esse plano tinha cinco etapas.

Jargão

CONEXÃO DIRETA A expressão da empresa de telefonia para uma linha telefônica que vai diretamente para um número específico quando o telefone é tirado do gancho.

NEGAR ENCERRAMENTO Uma opção de serviço da empresa de telefonia na qual o equipamento de comutação é definido para que as ligações não possam ser recebidas naquele número de telefone.

Primeiro, ele encontraria os números de telefone daqueles dez telefones de conexão direta com o EDP.

Mudaria todos os dez para que os telefones também pudessem receber ligações.

Descobriria em qual unidade estava Gondorff.

Em seguida, descobriria qual número de telefone ia para aquela unidade.

Finalmente, combinaria com Gondorff um momento para ele esperar a sua ligação, sem que o governo suspeitasse de nada.

Muito fácil, ele pensou.

Ligue para mim...

Johnny começou ligando para o escritório comercial da empresa de telefonia sob o pretexto de ser da Administração de Serviços Gerais, a agência responsável pela compra dos bens e serviços para o governo federal. Ele disse que estava trabalhando em um pedido de aquisição de serviços adicionais e precisava das informações de faturamento dos serviços de conexão direta usados no momento, incluindo os números de telefones e o custo mensal do centro de detenção de São Diego. A senhora ficou feliz em ajudar.

Só para ter certeza, tentou discar para uma daquelas linhas e obteve a gravação típica: "Esta linha foi desligada ou está fora de serviço no momento" — o que ele sabia que não significava nada além de que a linha estava programada para bloquear as ligações recebidas.

Ele sabia com o seu amplo conhecimento das operações e dos procedimentos da empresa de telefonia que precisava falar com um departamento chamado Centro de Autorização de Memória de Alterações Recentes ou RCMAC (sempre me pergunto quem será que inventa esses nomes!). Ele começou ligando para o Escritório de Negócios da empresa de telefonia. Disse que era de Consertos e precisava do número do RCMAC que tratava da área de serviço do código de área e prefixo que ele tinha, o qual era atendido pelo mesmo escritório central de todas as linhas telefônicas do centro de detenção. Essa era uma solicitação de rotina, o tipo de informação fornecida aos técnicos que estão de serviço e precisam de auxílio, e o operador não hesitou em lhe dar o número.

Ele ligou para o RCMAC, deu um nome falso e repetiu que trabalhava em Consertos. Quem atendeu foi a senhora que deu os números de telefone do centro de detenção algumas ligações antes. Quando ela atendeu, Johnny perguntou: "Esse é o número configurado para negar encerramento?"

"Sim", ela disse.

"Bem, isso explica por que o cliente não consegue receber ligações!", afirmou Johnny. "Ouça, você pode me fazer um favor? Preciso mudar o código de classe da linha ou remover o recurso para negar encerramento, tudo bem?" Houve uma pausa enquanto ela verificava outro sistema de computador para saber se um pedido de serviço havia sido feito para autorizar a mudança. Ela explicou: "Esse número *deve* estar restrito apenas para as ligações feitas. Não há nenhuma ordem de serviço para uma mudança."

"Certo, mas há um erro. Devíamos ter processado o pedido ontem, mas o representante normal da conta que trata desse cliente ficou doente e esqueceu de passar o pedido para outra pessoa. Assim sendo, agora é claro que o cliente está reclamando."

Após alguns momentos enquanto a senhora pensava na solicitação, o que iria contra os procedimentos operacionais padrão e comuns, ela disse: "OK". Ele a ouviu digitando a alteração. E alguns segundos depois estava tudo pronto.

O gelo havia sido quebrado, um tipo de cumplicidade havia sido estabelecido entre os dois. Lendo a atitude e disposição da mulher em ajudar, Johnny não hesitou em se aproveitar. Ele disse: "Você tem alguns minutos mais para me ajudar?"

"Sim", ela respondeu. "Do que você precisa?"

"Tenho algumas outras linhas do mesmo cliente, e todas estão com o mesmo problema. Vou ler os números para você conferir se eles não estão configurados para negar encerramento — tudo bem?" Ela disse que estava tudo bem.

Alguns minutos depois, todas as dez linhas telefônicas haviam sido "consertadas" para receber ligações.

Encontrando Gondorff

A seguir, ele precisava encontrar em qual alojamento estava Gondorff. Essas são aquelas informações que o pessoal que administra os centros de detenção e as prisões não quer que pessoas de fora saibam. Novamente Johnny teve de depender das suas habilidades de engenheiro social.

Ele fez uma ligação para a prisão federal de outra cidade — ligou para Miami, mas qualquer outra prisão serviria — e disse que estava ligando do centro de detenção de Nova York. Ele pediu para falar com alguém que trabalhasse no computador Sentry do Bureau, o sistema de computadores que contém as informações sobre todos os prisioneiros de uma instalação do Bureau de Prisões em qualquer lugar do país.

Quando aquela pessoa atendeu, Johnny caprichou no seu sotaque do Brooklyn. "Oi", ele começou. "Aqui é Thomas do FDC Nova York. A nossa conexão com o Sentry está caindo, você pode encontrar a localização de um prisioneiro para mim, acho que ele pode estar na sua instituição", e deu o nome e o número de registro de Gondorff.

"Não, ele não está aqui", o rapaz respondeu após alguns momentos. "Ele está no centro correcional de São Diego."

Johnny fingiu estar surpreso. "São Diego! Ele deveria ter sido transferido para Miami na semana passada! Será que estamos falando da mesma pessoa — qual é a data de nascimento dele?"

"3/12760", o homem leu na sua tela.

"Sim, é o mesmo. Em qual alojamento ele está?"

"Ele está no Dez Norte", disse o homem — respondendo a pergunta, muito embora não houvesse nenhum motivo para que um empregado de uma prisão de Nova York precisasse saber disso.

Johnny agora tinha os telefones acionados para receber ligações e sabia em qual unidade estava Gondorff. A seguir, tinha de descobrir qual número de telefone estava conectado à unidade Dez Norte.

Essa etapa era um pouco mais difícil. Johnny ligou para um dos números. Ele sabia que a campainha estaria desligada e ninguém saberia que ele estava tocando. Assim sendo, ficou lá sentado lendo o guia de viagem *Grandes Cidades da Europa* enquanto ouvia o sinal constante no fone de ouvido até que finalmente alguém atendeu. O interno do outro lado, obviamente, estava tentando falar com o seu advogado. Johnny estava preparado com a resposta esperada. "Escritório do Defensor Público", ele anunciou.

Quando o homem pediu para falar com o seu advogado, Johnny disse: "Vou ver se ele está disponível, de qual alojamento você está ligando?". Ele anotou a resposta do homem, colocou a ligação

em espera e voltou após meio minuto com a resposta: "Ele está no tribunal, você terá de ligar mais tarde", e desligou.

Ele havia passado uma boa parte da manhã, mas poderia ter sido pior; a sua quarta tentativa caiu no Dez Norte. Assim sendo, Johnny agora tinha o número de telefone com o EDP da unidade onde estava Gondorff.

Sincronizem seus relógios

Agora ele precisava mandar um recado para Gondorff dizendo para atender o telefone que conecta os internos diretamente com o Escritório do Defensor Público. Isso era mais fácil do que parecia.

Johnny ligou para o centro de detenção usando a sua voz "oficial", identificou-se como um empregado e pediu para ser transferido para o Dez Norte. A ligação foi completada imediatamente. Quando o oficial atendeu, Johnny o enganou usando a abreviação interna para Receber e Liberar, a unidade que processa os novos internos e libera aqueles que estão sendo soltos: "Aqui é Tyson do R&L", ele disse. "Preciso falar com o interno Gondorff. Temos alguns pertences dele e precisamos que ele nos dê o endereço para onde enviá-los. Você pode chamá-lo para mim ao telefone?"

Johnny ouviu o guarda gritando na sala de atividades diárias. Após vários minutos de impaciência, uma voz familiar atendeu.

Johnny disse: "Não diga nada até eu explicar do que se trata". Ele explicou a desculpa para que Johnny pudesse fingir que eles estavam discutindo para onde mandar os seus pertences. Johnny então prosseguiu: "Se você puder pegar o telefone com o Defensor Público à uma da tarde hoje, não responda. Se não puder, então diga uma hora que você estará lá." Gondorff não respondeu. Johnny continuou: "Bom. Esteja lá às treze horas. Vou ligar. Pegue o telefone. Se começar a cair no Escritório dos Defensores Públicos, desligue e ligue a cada vinte segundos. Continue tentando até me ouvir do outro lado."

As treze horas Gondorff pegou o telefone e Johnny estava lá esperando por ele. Eles conversaram animadamente e sem pressa, o que levou a uma série de ligações semelhantes para planejar o golpe que levantaria o dinheiro para pagar os honorários do advogado de Gondorff— tudo sem que o governo soubesse.

Analisando a trapaça

Esse episódio oferece um bom exemplo de como um engenheiro social pode fazer o que parece ser impossível acontecer enganando diversas pessoas, cada uma fazendo uma coisa que sozinha parece não ter conseqüências. Na verdade, cada ação fornece uma pequena parte do quebra-cabeça até que o golpe esteja completo.

A primeira funcionária da empresa de telefonia pensou que estava dando as informações para alguém do Escritório de Contabilidade Geral do governo federal. A próxima funcionária da empresa de telefonia sabia que não devia mudar a classe do serviço telefônico sem uma ordem de serviço, mas ajudou o homem amistoso de qualquer maneira. Isso possibilitou fazer ligações de todas as dez linhas telefônicas que ligam para o defensor público no centro de detenção.

Para o homem do centro de detenção de Miami, a solicitação de ajudar alguém de outra unidade federal com um problema de computador pareceu algo perfeitamente razoável. E embora não houvesse nenhum motivo para ele saber a unidade do alojamento, por que não responder à pergunta?

E o guarda do Dez Norte, que acreditava que o interlocutor estava falando realmente de dentro da mesma instalação, ligando em missão oficial? Essa era uma solicitação perfeitamente razoável, de modo que ele chamou o interno Gondorff para atender ao telefone. Nada muito fora do comum.

Uma série de histórias bem planejadas que resultaram na conclusão do golpe.

O DOWNLOAD MAIS RÁPIDO

Dez anos após ter terminado a faculdade de Direito, Ned Racine via seus colegas de classe morando em belas casas com jardins na frente, associados de country clubs, jogando golfe uma ou duas vezes por semana, enquanto ele ainda estava cuidando de causas baratas para o tipo de pessoa que nunca tinha dinheiro suficiente para pagar a conta. O ciúme pode ser uma má companhia. Finalmente, um dia Ned ficou farto daquilo tudo.

O único bom cliente que já tivera era uma empresa de contabilidade pequena, mas bem-sucedida, especializada em incorporações e aquisições. Há muito tempo eles não usavam os serviços de Ned, o suficiente para ele perceber que eles estavam envolvidos em negócios que, depois de chegarem aos jornais, afetariam o preço das ações de uma ou duas empresas públicas. As ações valiam pouco, **mas** de alguma maneira isso era melhor ainda — um pequeno aumento no preço representaria uma grande porcentagem de lucro sobre o investimento. Se ele pudesse acessar seus arquivos e descobrir no que eles estavam trabalhando...

Ele conhecia um homem que tinha experiência em coisas que não seguem exatamente o procedimento padrão. O homem ouviu o plano, interessou-se e concordou em ajudar. Por uma taxa mais baixa do que aquela que é cobrada normalmente, mais uma porcentagem sobre as ações de Ned. o homem deu as instruções sobre o que ele deveria fazer. Ele também lhe deu um conselho útil, algo totalmente novo no mercado.

Durante alguns dias seguidos, Ned observou o estacionamento onde a pequena empresa de contabilidade tinha o despretensioso escritório do tipo loja. A maioria das pessoas saía entre 17h30 e 18h. Às 19h o estacionamento estava vazio. O pessoal da limpeza aparecia por volta das 19h30. Perfeito! [

Na noite seguinte, alguns minutos antes das 20h, Ned estacionou do outro lado da rua em frente ao estacionamento. Como esperava, o estacionamento estava vazio, exceto pelo caminhão da empresa de serviços de limpeza. Ned colocou o ouvido na porta e ouviu o aspirador de pó funcionando. Ele bateu na porta com força e ficou esperando em seu terno e gravata e segurando a pasta. Nenhuma resposta, mas ele era paciente. Ele bateu novamente. Um homem do pessoal da limpeza finalmente apareceu. "Oi", Ned gritou pela porta de vidro, mostrando o cartão de visitas de um dos sócios que ele havia pego algum tempo antes. "Tranquei as minhas chaves no carro e preciso ir até a minha mesa."

O homem abriu a porta, trancou-a novamente depois que Ned entrou e passou pelo corredor acendendo as luzes para que Ned pudesse ver aonde estava indo. E por que não — ele estava sendo gentil com uma das pessoas que o ajudava a colocar comida na mesa. Ou pelo menos ele tinha todos os motivos para pensar isso.

Ned sentou-se no computador de um dos sócios e o ligou. Enquanto o computador inicializava, ele instalou o pequeno dispositivo na porta USB do computador, um dispositivo suficientemente pequeno para ser transportado em um chaveiro, mas capaz de conter mais de 120 megabytes de dados. Ele se conectou à rede usando o nome de usuário e a senha da secretária do sócio, os quais estavam convenientemente escritos em uma anotação colada na tela. Em menos de cinco minutos, Ned havia

descarregado todas as planilhas e arquivos de documentos armazenados na estação de trabalho e no diretório de trabalho do sócio e foi para casa.

Recado do Mitnick

Os espiões industriais e invasores de computador eventualmente fazem uma entrada física na empresa-alvo. Em vez de usar um pé de cabra para quebrar a porta, o engenheiro social usa a arte da fraude para influenciar a pessoa que está do outro lado da porta para abri-la para ele.

DINHEIRO FÁCIL

Quando fui apresentado aos computadores pela primeira vez no colégio, tínhamos de nos conectar por modem a um minicomputador DEC PDP 11 no centro da cidade de Los Angeles. Todos os colégios de Los Angeles compartilhavam desse mesmo minicomputador. O sistema operacional daquele Computador se chamava RSTS/E e esse foi o primeiro sistema operacional com o qual aprendi a trabalhar.

Naquela época, em 1981, a DEC patrocinava uma conferência anual para seus usuários de produto, e um ano li que a conferência seria realizada em Los Angeles. Uma revista conhecida para os usuários desse sistema operacional trazia um anúncio sobre um novo produto de segurança, o LOCK-11. O produto era promovido com uma campanha publicitária inteligente que dizia algo do tipo "São 3h30 da manhã e Johnny, do final da rua, descobriu o seu número de discagem. 555-0336, na sua 336ª. tentativa. Ele está dentro e você está fora. Use o LOCK-11". O anúncio sugeria que o produto era à prova de hackers. E ele seria exibido na conferência.

Eu estava ansioso para ver o produto. Um colega e amigo do colégio, Vinny, meu parceiro de hacking durante vários anos e que se tornou mais tarde um informante dos federais contra mim, compartilhava do meu interesse no novo produto da DEC e me incentivou a ir à conferência com ele.

Dinheiro on-line

Chegamos lá e encontramos um grande movimento das pessoas que estavam na feira ao redor do LOCK-11. Parece que os desenvolvedores estavam apostando dinheiro on-line para ver quem conseguia quebrar a segurança do produto. Esse parecia um desafio ao qual eu não poderia resistir.

Fomos direto ao stand do LOCK-11 e encontramos os três desenvolvedores do produto. Eu os reconheci e eles me reconheceram —- mesmo adolescente eu já tinha fama de phreaker e hacker por causa de um artigo que o *LA Times* havia publicado sobre meu primeiro contato juvenil com as autoridades. O artigo relatava que eu havia entrado no prédio da Pacific Telephone no meio da noite e tirado manuais de computadores, bem debaixo do nariz dos guardas de segurança. (Parece que o *Times* queria criar uma história sensacionalista e a publicação do meu nome servia para isso; como eu era ainda um adolescente, o artigo violou a prática, senão a lei, de não-divulgação dos nomes dos menores acusados de infrações.)

Quando Vinny e eu chegamos, isso criou um certo interesse de ambos os lados. Havia um interesse da parte deles porque eles me reconheceram como o hacker sobre quem haviam lido e eles estavam um pouco chocados em me ver. Isso criou um interesse também da nossa parte, porque cada

um dos três desenvolvedores eslava lá com uma nota de US$ 100 pendurada no crachá da exposição. O prêmio em dinheiro total para todos que pudessem invadir seu sistema seria de US$ 300 — o que parecia bastante dinheiro para uma dupla de adolescentes. Mal podíamos esperar para começar.

O LQCK-11 foi criado com base em um princípio estabelecido que dependia de dois níveis de segurança. Um usuário precisava ter um ID e uma senha válida, como sempre, mas o ID e a senha só funcionariam quando fossem inseridos em terminais autorizados, uma abordagem chamada de *segurança baseada em terminal.* Para burlar o sistema, um hacker precisaria não apenas ter um ID de conta e uma senha, mas também teria de inserir essas informações no terminal correto. O método estava bem estabelecido e os inventores do LOCK-11 estavam convencidos de que isso manteria as pessoas más de fora. Nós resolvemos que iríamos ensinar uma lição para eles e embolsar as 300 pratas.

Um rapaz que eu conhecia e que era considerado um guru do RSTS/E já havia nos derrotado. Anos antes ele tinha me desafiado a entrar no computador interno de desenvolvimento da DEC, e depois disso seus colegas me entregaram. Desde aquela época ele havia se tornado um programador respeitado. Nós descobrimos que ele havia tentado burlar o programa de segurança LOCK-11 pouco antes de chegarmos, mas não conseguiu. O incidente havia dado aos desenvolvedores mais segurança de que o seu produto realmente era seguro.

O concurso era um grande desafio: vencer o sistema de segurança e levar o dinheiro. Um bom golpe publicitário... a menos que alguém conseguisse e levasse o dinheiro. Eles tinham tanta certeza de que o seu produto era seguro que até se atreveram a afixar no stand uma lista com os números e senhas de algumas das contas do sistema. E não apenas as contas comuns, mas também as contas privilegiadas.

Na verdade, isso era menos audacioso do que parecia. Eu sabia que nesse tipo de configuração cada terminal está conectado a uma porta do próprio computador. Não era preciso ser um cientista aeroespacial para descobrir que eles haviam configurado cinco terminais na sala de reuniões para que um visitante fizesse a conexão apenas como um usuário não privilegiado — ou seja, os logins só eram possíveis para as contas que não tinham privilégios de administradores de sistemas. Parecia que havia apenas duas rotas: desviar totalmente do software de segurança — exatamente aquilo que o LOCK-11 deveria evitar, ou burlar o software de alguma maneira que os desenvolvedores não haviam imaginado.

Aceitando o desafio

Vinny e eu fomos dar uma volta para conversar sobre o desafio e voltamos com um plano. Ficamos por ali inocentemente e vigiamos o stand à distância. Na hora do almoço, quando o movimento diminuiu, os três desenvolvedores se aproveitaram do intervalo e saíram juntos para comer alguma coisa, deixando lá uma mulher que poderia ser a mulher ou namorada de um deles. Nós voltamos e eu distrai a mulher, conversando com ela sobre várias coisas como "Há quanto tempo você trabalha na empresa?", "Quais outros produtos a sua empresa vende?" e assim por diante.

Jargão

SEGURANÇA BASEADA EM TERMINAL A segurança baseada em parte na identificação do terminal de computador específico que está sendo usado. Esse método de segurança era particularmente conhecido nos computadores mainframe da IBM.

Nesse meio tempo, Vinny, que estava fora da sua linha de visão, estava trabalhando, usando uma habilidade que nós dois havíamos desenvolvido. Além do fascínio por invadir computadores e do meu próprio interesse em mágica, uma coisa que sempre nos interessou foi aprender como abrir cadeados. Quando criança, eu havia percorrido as prateleiras de uma livraria obscura no Vale de São Fernando, que tinha livros sobre como abrir cadeados, livrar-se de algemas, criar identidades falsas — todo o tipo de coisas que uma criança não deveria saber.

Assim como eu, Vinny havia praticado o arrombamento de cadeados até ficarmos muito bons nos cadeados comuns que se compram nas lojas de ferragens. Certa vez me diverti encontrando alguém que usava dois cadeados como uma medida extra de proteção. Eu troquei os cadeados de lugar, o que irritaria e frustraria o proprietário quando ele tentasse abrir cada um deles com a chave errada.

No recinto de exposições eu continuava distraindo a mulher enquanto Vinny se esgueirava na parte de trás do stand para não ser visto e pegava o cadeado do gabinete que abrigava o seu mini-computador PDP-11 e os terminais dos cabos. Dizer que o gabinete estava trancado era quase piada. Ele estava fechado com aqueles cadeados chamados de cadeado de biscoito, evidentemente fáceis de abrir até mesmo para arrombadores amadores como nós.

Vinny precisou de apenas um minuto para abrir o cadeado. Dentro do gabinete ele encontrou o que havia previsto: a fila de portas para conectar os terminais de usuários e uma porta para aquele que era chamado de terminal da console. Esse era o terminal usado pelo operador do computador ou administrador do sistema para controlar todos os computadores. Vinny conectou o cabo que ia da porta da console até um dos terminais da feira.

Isso significava que esse terminal agora era reconhecido como o terminal da console. Eu me sentei na máquina com os cabos novos e me conectei usando uma senha que os desenvolvedores haviam fornecido. Como o software LOCK-11 agora identificava que eu estava me conectando de um terminal autorizado, ele me concedeu o acesso e eu estava conectado com privilégios de administrador de sistema. Fiz o patch do sistema operacional para que eu pudesse me conectar como usuário privilegiado de qualquer terminal do local.

Depois que o meu patch secreto estava instalado, Vinny voltou a trabalhar desconectando o cabo de terminal e conectando-o de volta no lugar onde ele estava originalmente. Em seguida pegou o cadeado mais uma vez, desta vez para trancar a porta do gabinete.

Pedi uma listagem de diretórios para saber quais arquivos havia no computador, procurei o programa LOCK-11 e os arquivos associados e encontrei algo que achei chocante: um diretório que não deveria estar naquela máquina. Os desenvolvedores estavam tão confiantes, tão certos de que seu software era invencível que nem se importaram em remover o código-fonte do novo produto. Fui até o terminal de impressão ao lado e comecei a imprimir partes do código-fonte nas folhas de formulário contínuo com listras verdes que eram usadas naquela época.

Vinny havia acabado de fechar o cadeado e tinha se juntado a mim quando os desenvolvedores voltaram do almoço. Eles me encontraram sentado no computador digitando enquanto a impressora continuava trabalhando. "O que você está fazendo, Kevin?", um deles me perguntou.

"Ah, só estou imprimindo o seu código-fonte", respondi. Eles pensaram, é claro, que eu estava brincando. Até que olharam a impressora e viram que aquilo realmente *era* o código-fonte tão bem guardado do seu produto.

Eles não acreditaram que eu estivesse conectado como usuário privilegiado. "Digite um Control-T", ordenou um dos desenvolvedores. Eu fiz isso. A tela confirmou o que eu disse. O rapaz começou a bater na cabeça enquanto Vinny pedia: "Os US$ 300, por favor".

Recado do Mitnick

Este é outro exemplo de pessoas inteligentes que subestimam o inimigo. E você? Você tem tanta certeza de que a sua empresa está segura a ponto de apostar US$300 como um atacante não pode invadi-la? Às vezes o modo de contornar um dispositivo de segurança não é aquele que se espera.

Eles pagaram. Vinny e eu caminhamos pela exposição no restante do dia com as notas de US$ 100 pregadas em nossos crachás da conferência. Todos que viam as notas sabiam o que elas representavam.

Obviamente, Vinny e eu burlamos o software deles, e se a equipe de desenvolvedores tivesse pensado em definir regras melhores para o concurso, se tivessem usado um cadeado realmente seguro ou se tivessem tomado conta do seu equipamento com mais cuidado não teriam sofrido aquela humilhação naquele dia — a humilhação sofrida pelas mãos de dois adolescentes.

Mais tarde descobri que a equipe de desenvolvedores teve de ir ao banco para tirar dinheiro: aquelas notas de US$ 100 eram todo o dinheiro que tinham com eles para gastar.

O DICIONÁRIO COMO UMA ARMA DE ATAQUE

Quando alguém consegue a sua senha, essa pessoa pode invadir o seu sistema. Na maior parte dos casos, você nem sabe que alguma coisa ruim aconteceu.

Um atacante jovem que chamarei de Ivan Peters tinha como alvo recuperar o código-fonte de um novo jogo eletrônico. Ele não teve problemas para entrar na rede remota da empresa, porque um colega hacker já havia comprometido um dos servidores Web da empresa. Após encontrar uma vulnerabilidade sem patch no software do servidor Web, esse colega quase caiu da cadeira quando percebeu que o sistema havia sido configurado como *host dual-homed*, o que significa que ele tinha um ponto de entrada para a rede interna.

Depois que Ivan se conectou, ele enfrentou um desafio que era como estar dentro do Louvre e esperar encontrar a Mona Lisa. Sem a planta do local você pode passar semanas perambulando. A empresa era global, com centenas de escritórios e milhares de servidores de computador, e eles não forneciam um índice dos sistemas de desenvolvimento ou um serviço de guia para orientá-lo até o sistema certo.

Em vez de usar uma abordagem técnica para descobrir qual seria o servidor-alvo, Ivan usou uma abordagem da engenharia social. Ele fez ligações telefônicas com base em métodos semelhantes àqueles descritos neste livro. Em primeiro lugar, ligou para o suporte técnico de TI e disse ser um empregado da empresa que tinha um problema de interface em um produto que o seu grupo estava desenvolvendo, e pediu o número de telefone do líder de projeto da equipe de desenvolvimento de jogos.

Em seguida, ligou para a pessoa cujo nome lhe deram e fingiu ser um funcionário de TI. "No final desta noite", ele disse, "vamos trocar um roteador e precisamos ter certeza de que o pessoal da nossa equipe não vai perder a conectividade com o seu servidor. Assim sendo, precisamos saber quais servidores a sua equipe usa". A rede estava sempre sendo atualizada. E dar o nome do servidor não causaria dano nenhum, não é? Como ele eslava protegido por senha, apenas o nome não adiantaria

para alguém que quisesse invadir o sistema. Assim sendo, a vítima deu ao atacante o nome do servidor. Ele nem se importou de ligar para o homem de volta e verificar a história, nem tampouco anotou o seu nome e número de telefone. Ele apenas deu o nome dos servidores, ATM5 e ATM6.

O ataque da senha

Nesse ponto, Ivan usou uma abordagem técnica para obter as informações de autenticação. A primeira etapa da maioria dos ataques técnicos a sistemas que fornecem a capacidade de acesso remoto *é* a identificação de uma conta com uma senha fraca, a qual fornece um ponto de entrada inicial para o sistema.

Quando um atacante tenta usar as ferramentas de hacking para identificar remotamente as senhas, o esforço pode exigir que ele permaneça conectado à rede da empresa durante horas de cada vez. E claro que ele está correndo risco: quanto mais tempo permanecer conectado, maior será o risco de ele ser pego.

Como etapa preliminar, Ivan faria uma *enumeração,* a qual revela os detalhes sobre um sistema-alvo. Novamente a Internet fornece software para essa finalidade (em http://ntsleuth.Ocatch.com; o caractere antes de "catch" é um zero). Ivan descobriu diversas ferramentas públicas de hacking na Web que automatizavam o processo de enumeração e evitavam a necessidade de fazer isso à mão, o que levaria mais tempo e aumentaria o risco. Sabendo que a organização empregava principalmente servidores baseados no Windows, ele baixou uma cópia do NBTEnum, um utilitário de enumeração do **NetBIOS** (sistema básico). Entrou com o endereço IP (protocolo Internet) do servidor ATM5 e começou a executar o programa. A ferramenta de enumeração podia identificar as diversas partições, contas e diretórios que existiam no servidor.

Após a identificação das contas existentes, a mesma ferramenta de enumeração podia iniciar um ataque de dicionário contra o sistema de computadores. Um ataque de dicionário é algo que muitas pessoas ligadas à segurança de computadores e intrusos conhecem bem. mas a maioria das outras pessoas provavelmente fica chocada quando descobre que isso é possível. Tal ataque visa descobrir a senha de cada usuário do sistema usando as palavras mais comuns.

Todos temos preguiça de fazer algumas coisas, mas sempre me surpreendo com o modo como as pessoas escolhem suas senhas, quando a sua criatividade e imaginação parecem desaparecer. A maioria de nós quer um3 senha que de proteção, mas que ao mesmo tempo seja fácil de lembrar, o que significa algo que esteja muito ligado a nós mesmos. As iniciais do nosso nome, o nome do meio, o apelido, o nome do esposo, a canção preferida, filme ou marca de café, por exemplo. O nome da rua em que moramos ou da cidade em que vivemos, a marca do carro que dirigimos, a praia na qual gostamos de ficar no Havaí ou aquele riacho preferido com a melhor truta que pode ser pescada. Você reconhece um padrão aqui? Em sua maioria essas senhas são nomes de pessoas, nomes de lugares ou palavras do dicionário. Um ataque de dicionário procura as palavras comuns com velocidade grande e experimenta cada senha em uma ou mais contas de usuário.

Jargão

ENUMERAÇÃO Um processo que revela os serviços que estão ativos no sistema-alvo, a plataforma do sistema operacional e uma lista dos nomes de contas dos usuários que têm acesso ao sistema.

Ivan executou o ataque de dicionário em três fases. Na primeira fase, usou uma lista simples com algumas das 800 senhas mais comuns; a lista incluía *segredo, trabalho* e *senha.* O programa também trocava as palavras do dicionário para experimentar cada palavra com um dígito anexado, ou anexando o número do mês atual. O programa tentava a cada instante descobrir a senha em todas as contas de usuário que haviam sido identificadas. Entretanto, ele não teve sorte.

Na próxima tentativa, Ivan foi ao mecanismo de pesquisa do Google e digitou "arquivos-dicionários" e encontrou milhares de sites com listas de palavras e dicionários em inglês e em diversos idiomas estrangeiros no formato texto. Ele fez o download de todo um dicionário eletrônico do idioma inglês. Em seguida, aumentou esse dicionário, fazendo o download de várias listas de palavras que encontrou com o Google. Ivan escolheu o site em www.outpost9.com/files/WordLists.html.

Esse site permitiu que ele fizesse o download (tudo isso *de graça)* de uma série de arquivos, incluindo nomes de família, nomes dados, nomes e palavras do Congresso, nomes de atores, palavras e nomes da Bíblia.

Outro site que fornece listas de palavras é o site da Oxford University, em ftp://ftp.ox.ac.uk/pub/wordlists.

Outros sites oferecem listas com nomes de personagens de quadrinhos, palavras usadas nos textos de Shakespeare, nas séries Odyssey, Tolkien e Star Trek, bem como palavras das áreas de ciências e religião e assim por diante. (Uma empresa on-line vende uma lista contendo 4,4 milhões de palavras e nomes por apenas US$ 20.) O programa de ataque também pode ser definido para testar anagramas das palavras do dicionário — outro método favorito de muitos usuários de computador que acham que estão aumentando a sua segurança dessa forma.

Mais rápido do que o pensamento

Depois que Ivan resolveu qual lista de palavras usaria e começou o ataque, o software foi executado no piloto automático. Ele pode voltar a sua atenção para outras coisas. E aqui está a parte mais inacreditável. Você acha que esse ataque permite a um hacker dar a volta ao mundo e o software ainda teria feito pouco progresso quando ele voltasse? Na verdade, dependendo da plataforma que está sendo atacada, da configuração de segurança do sistema e da conectividade de rede, cada palavra de um dicionário do inglês pode, acredite ou não, ser testada em menos de cinco segundos!

Enquanto esse ataque estava em execução, Ivan ligou outro computador para executar um ataque semelhante a outro servidor usado pelo grupo de desenvolvimento, o ATM6. Vinte minutos depois o software de ataque havia feito aquilo que os usuários mais crédulos gostam de achar que é impossível: ele havia encontrado uma senha que revelava que um dos usuários havia escolhido a palavra "Frodo", um dos Hobbits do livro *O Senhor dos Anéis.*

Com essa senha Ivan pode se conectar ao servidor ATM6 usando a conta do usuário.

Havia uma boa e uma má notícia para o nosso atacante. A boa notícia era que a conta que ele invadira tinha privilégios de administrador, o que seria essencial para a próxima etapa. A má notícia era que o código-fonte do jogo não estava em nenhum lugar. Ele devia estar em outra máquina, a ATM5, e ele já sabia que ela era resistente a um ataque de dicionário. Mas Ivan ainda não desistira, ele ainda tinha mais alguns truques para experimentar.

Em alguns sistemas operacionais Windows e UNIX, os hashes de senha (as senhas criptografadas) estão disponíveis para todos que tenham acesso ao computador no qual eles estão armazenados. O raciocínio é que as senhas criptografadas não podem ser descobertas e, portanto, não precisam estar

protegidas. Essa teoria está errada. Usando outra ferramenta chamada pwdump3. a qual também está disponível na Internet, ele pôde extrair os hashes de senha da máquina ATM6 e fez o seu download.

Um arquivo típico de hashes de senhas se parece com este:

Administrator: 500:95E4321A38AD8D6AB7SE0C8D76954A50 :2E48927A0 B04F3BFB341E26F6D6E9A97 : : :

akasper: 1110 : 5A8D7E9E3C3 954F64 2C5C736306CBFEF : 393CE7F90A8357 F157873D72D0490821 : : :

digger: 1111 : 5D15C0D58DD2 16C525AD3B83FA6627C7 : 17AD564144308B4 2B8403D01AE256558 : : :

ellgan: 1112 : 2017D4A5D8D1383EFF17365FAFlFFE89 : 07AEC950C22CBB9 C2C734EB89320DB13 : : :

tabeck : 1115 : 9F5890B3FECCAB7EAAD3B4 35B51404EE : 1F0115A72844721 2FC05E1D2D820B35B:::

vkantar: 1116 : 8 1A6A5D035596E7DAAD3B435B51404EE : B933D36DD12258 946FCC7BD153F1CD6E : : :

vwallwick :1119 : 25904EC665BA30F4449AF42E1054F192 : 15B2B7953FB6 32907455D2706A432469 : : :

mmcdonald: 1121 : A4AED098D2 9A3217AAD3B435B51404EE : E40670F936B7 9C2ED522F5ECA9398A27: : :

kworkman : 1141 : C5C598AF45768635AAD3B435B51404EE : DEC8E827A1212 73EF084CDBF5FD1925C : : :

Agora com o download dos hashes no seu computador. Ivan usou outra ferramenta que executava um tipo diferente de ataque de senha conhecido *como força bruta.* Esse tipo de ataque tenta todas as combinações de caracteres alfanuméricos e os símbolos mais especiais.

Ivan usou um utilitário de software chamado L0phtcrack3 (loft crack o qual está disponível em www.atstake.com; outra fonte de algumas ferramentas excelentes para a recuperação de senhas é www.elcomsoft.com). Os administradores de sistema usam o L0phtcrack3 para fazer a auditoria das senhas fracas; os atacantes o usam para descobrir senhas. O recurso de força bruta do LC3 tenta as senhas com combinações de letras, numerais e a maioria dos símbolos incluindo !@#$%^&. Ele tenta sistematicamente todas as combinações possíveis da maioria dos caracteres. (Observe, porém, que se forem usados os caracteres não impressos, o LC3 não pode descobrir a senha.)

O programa tem uma velocidade quase inacreditável, a qual pode chegar a até 2,8 milhões de tentativas por segundo em uma máquina com um processador de 1 GHz. Mesmo com essa velocidade e se o administrador de sistema configurou o sistema operacional Windows adequadamente (desativando o uso dos hashes LANMAN), a descoberta de uma senha pode levar um tempo excessivo.

Por esse motivo o atacante quase sempre faz o download dos hashes e executa o ataque em sua própria máquina ou em outra, em vez de ficar on-line na rede da empresa-alvo e se arriscar a ser pego.

Jargão

ATAQUE DE FORÇA BRUTA **Uma estratégia de descoberta de senha que tenta todas as combinações possíveis de caracteres alfanuméricos e símbolos especiais.**

Para Ivan a espera não foi tão longa. Várias horas mais tarde o programa apresentou as senhas de cada um dos membros da equipe de desenvolvimento. Mas essas eram as senhas dos usuários da máquina ATM6 e ele já sabia que o código-fonte do jogo que desejava não estava nesse servidor.

E agora? Ele ainda não conseguira uma senha para uma conta da máquina ATM5. Usando o seu raciocínio de hacker e sabendo dos maus hábitos de segurança dos usuários em geral, ele calculou que um dos membros da equipe poderia ter escolhido a mesma senha em ambas as máquinas.

Na verdade foi exatamente isso o que aconteceu. Um dos membros da equipe usava a senha "jogadores" no ATM5 e no ATM6.

A porta havia se escancarado para Ivan caçar até encontrar o programa que procurava. Após localizar o diretório do código-fonte e fazer o seu download, ele executou outra etapa típica dos invasores de sistemas: mudou a senha de uma conta inativa que tinha direitos administrativos, só para o caso de querer obter uma versão atualizada do software no futuro.

Analisando a trapaça

Nesse ataque, que explorava as vulnerabilidades técnicas e pessoais, o atacante começou com uma ligação telefônica para obter a localização e os nomes dos hosts dos servidores de desenvolvimento que mantinham as informações proprietárias.

Em seguida, ele usou um utilitário de software para identificar os nomes de usuário de contas válidas de todos que tinham acesso ao servidor de desenvolvimento. A seguir, ele executou dois ataques sucessivos de senhas, entre eles um ataque de dicionário, o qual pesquisa as senhas mais usadas tentando todas as palavras de um dicionário da língua inglesa, às vezes aumentado por diversas listas de palavras contendo nomes, locais e itens de interesse especial.

Como as ferramentas de hacking comerciais e de domínio público podem ser obtidas por qualquer pessoa para qualquer finalidade, é muito importante que você fique atento e proteja os sistemas de computadores da empresa e a sua infra-estrutura de rede.

A magnitude dessa ameaça não pode ser subestimada. De acordo com a revista *ComputerWorld*, uma análise nos escritórios de Nova York da Oppenheimer Funds levou a uma descoberta surpreendente. O vice-presidente da empresa para Segurança de Rede e Recuperação de Desastres executou um ataque de senhas contra os empregados de sua empresa usando um dos pacotes de software-padrão. A revista informou que em *três minutos* ele conseguiu descobrir as senhas de 800 empregados.

Recado do Mitnick

Na terminologia do jogo Monopoly, não use palavra do dicionário. Você tem de ensinar seus empregados como eles devem escolher senhas que protegem realmente os seus bens.

EVITANDO A TRAPAÇA

Os ataques da engenharia social podem se tornar ainda mais destrutivos quando o atacante usa um elemento de tecnologia. Para evitar esse tipo de ataque em geral você precisa seguir etapas nos níveis humano e técnico.

Diga simplesmente não

Na primeira história do capítulo, a funcionária da empresa de telefonia RCMAC não deveria ter removido o status "negar encerramento" das dez linhas telefônicas sem nenhuma ordem de serviço que autorizasse-a mudança. Não basta que os empregados *conheçam* as políticas e os procedimentos de segurança. Eles devem entender como essas políticas são importantes para evitar danos para a empresa.

As políticas de segurança devem desencorajar o desvio do procedimento por meio de um sistema de recompensas. Naturalmente, as políticas devem ser realistas e não devem pedir que os empregados executem etapas complicadas demais, caso contrário elas podem ser ignoradas. Da mesma forma, um programa de conscientização sobre a segurança precisa convencer os empregados que, embora seja importante realizar as tarefas da função dentro do prazo, a tomada de um atalho que não atende os procedimentos adequados de segurança pode ser prejudicial para a empresa e os colegas.

O mesmo cuidado deve ser tomado quando se fornecem informações para um estranho ao telefone. Não importa se a pessoa se apresenta de modo persuasivo, não importa o seu status ou a sua posição na hierarquia da empresa: *nenhuma* informação deve ser fornecida além daquelas designadas como publicamente disponíveis até que a identidade do interlocutor seja verificada positivamente. Se essa política fosse observada rigidamente, o esquema da engenharia social da história de Johnny teria falhado e Gondorff nunca poderia planejar um novo golpe com o seu colega Johnny.

Essa é uma questão tão importante que a reitero em todo este livro: verifique, verifique e verifique novamente. Toda solicitação que não seja feita pessoalmente nunca deve ser aceita sem a verificação da identidade do solicitante, ponto.

Fazendo a limpeza

Para todas as empresas que não têm pessoal de segurança durante as 24 horas do dia, o esquema no qual um atacante tem acesso a um escritório após o expediente representa um desafio. O pessoal da limpeza normalmente trata com respeito todos que aparentam trabalhar na empresa e pareçam ser verdadeiros. Afinal de contas, essa pessoa pode causar-lhes problemas ou sua demissão. Por esse motivo, as equipes de limpeza, sejam elas internas ou contratadas em uma agência externa, devem ser treinadas nas questões da segurança física.

O trabalho de limpeza não exige formação superior, nem mesmo a habilidade de falar fluentemente o idioma do país, e o treinamento normal, quando há, envolve questões não relacionadas com a segurança, tais como o tipo de produto de limpeza a ser usado para as diferentes tarefas. Em geral essas pessoas não são instruídas para "se alguém pedir para entrar fora do expediente você precisa verificar o cartão de identificação da empresa e, em seguida, ligar para o escritório da empresa de limpeza, explicar a situação e aguardar a autorização".

Uma organização precisa ter planos para uma situação como aquela deste capítulo antes que ela aconteça e treinar as pessoas adequadamente. De acordo com a minha experiência pessoal, descobri que a maioria das empresas (senão todas) do setor privado é muito relapsa nessa área da segurança física. Você pode tentar abordar o problema de outro modo, colocando a responsabilidade nos próprios empregados da sua empresa. Uma empresa sem serviço de segurança durante 24 horas deve dizer aos seus empregados que entram fora do expediente que eles devem levar suas próprias chaves ou cartões de acesso eletrônico e nunca devem colocar o pessoal da limpeza em uma situação em que eles tenham de resolver quem deve ser admitido. Em seguida, a empresa de limpeza deve ser avisada

que o seu pessoal de limpeza sempre deve ser treinado para não deixar ninguém entrar nas instalações da empresa em nenhum momento. Essa é uma regra simples: não abra a poria para ninguém. Se for apropriado, ela pode ser escrita como uma condição do contrato com a empresa de limpeza.

Da mesma forma, as equipes de limpeza devem ser treinadas quanto às técnicas usadas pelas pessoas não autorizadas que seguem uma pessoa autorizada quando ela passa pela entrada de segurança. Elas também devem ser treinadas para não permitir que outra pessoa as siga e entre no prédio só porque parece ser um empregado.

Faça um acompanhamento constante — digamos de três a quatro vezes por ano — realizando um teste de penetração ou uma avaliação de vulnerabilidade. Faça com que alguém apareça na porta quando a equipe de limpeza estiver trabalhando e tente entrar no prédio. Em vez de usar os seus próprios empregados, você pode contratar uma empresa especializada nesse tipo de teste de penetração.

Passe adiante: protejam suas senhas

Cada vez mais as organizações estão se tornando vigilantes sobre a implantação das diretivas lógicas de segurança — por exemplo, a configuração do sistema operacional para implantar as políticas de senhas e limitar o número de tentativas inválidas de login que podem ser feitas até que a conta seja bloqueada. Na verdade, as plataformas de negócios do Microsoft Windows geralmente têm esse recurso incorporado. Mesmo assim, reconhecendo o modo como os clientes se aborrecem facilmente com os recursos que exigem um esforço extra, os produtos são entregues na sua forma padrão, ou seja, com os recursos de segurança desativados. Está na hora de os fabricantes de software pararem de entregar produtos com os recursos na forma-padrão, pois deveria acontecer justamente o contrário. (Suspeito de que eles vão descobrir isso em breve.)

Obviamente, a política de segurança corporativa deve obrigar os administradores de sistema a implantarem diretivas lógicas de segurança sempre que possível, com o objetivo de não depender das pessoas não mais do que o necessário. Não é preciso pensar muito para ver que quando limita o número de tentativas sucessivas e inválidas de login com determinada conta, por exemplo, você torna a vida de um atacante significativamente mais difícil.

Toda organização enfrenta esse desconfortável desequilíbrio entre uma segurança forte e a produtividade do empregado, o qual faz com que alguns empregados ignorem as políticas de segurança e não aceitem o fato de que essas medidas são importantes para proteger a integridade das informações corporativas confidenciais.

Se as políticas de uma empresa não abordam algumas questões, os empregados podem usar o caminho da menor resistência e realizar as ações mais convenientes que tornem seu trabalho mais fácil. Alguns empregados podem resistir à mudança e ignorar os bons hábitos de segurança. Você talvez tenha encontrado um empregado assim, o qual segue as regras sobre o tamanho e a complexidade da senha, mas depois escreve a mesma senha em um Post-it e a cola no monitor.

Uma parte vital da proteção da sua organização é o uso de senhas difíceis de serem descobertas, as quais são combinadas a configurações rígidas de segurança na sua tecnologia. Consulte o Capítulo 16 para obter uma discussão detalhada sobre as políticas recomendadas de senhas.

Capítulo 12

Ataques aos Empregados Iniciantes

Como demonstram muitas histórias deste livro, o engenheiro social habilidoso quase sempre visa o pessoal de nível mais baixo da hierarquia organizacional. Pode ser fácil manipular essas pessoas para que elas revelem informações aparentemente inofensivas que o atacante usa para chegar mais próximo da obtenção das informações mais confidenciais da empresa.

Um atacante visa os empregados do nível iniciante porque geralmente eles não têm consciência do valor das informações específicas da empresa ou dos possíveis resultados de determinadas ações. Da mesma forma, eles tendem a ser facilmente influenciados por algumas das abordagens mais comuns da engenharia social — um interlocutor que invoca a autoridade; uma pessoa que parece amistosa e agradável; uma pessoa que parece conhecer pessoas da empresa que são conhecidas da vítima; uma solicitação que o atacante diz ser urgente ou a sugestão de que a vítima obterá algum tipo de favor ou reconhecimento.

Estas são algumas histórias de ataque ao empregado de nivel mais baixo em ação.

O GUARDA DE SEGURANÇA PRESTATIVO

Os ladrões esperam encontrar uma pessoa ambiciosa porque são elas que têm mais chances de cair em um jogo de trapaça. Os engenheiros sociais, quando visam alguém, tal como um membro de uma equipe de limpeza ou um guarda da segurança, esperam encontrar um indivíduo de boa índole, amistoso e que confia nas outras pessoas. Eles são aqueles que têm mais chances de estarem dispostos a ajudar. É exatamente isso o que o atacante da próxima história tem em mente.

A visão de Elliot

Data/hora: 3h26 da madrugada de terça-feira em fevereiro de 1998.

Localização: instalações da Marchand Microsystems, Nashua, New Hampshire

Elliot Staley sabia que não deveria sair do seu posto quando não estava nas rondas programadas, Mas ele estava no meio da noite e, para dizer a verdade, ainda não tinha visto uma única pessoa desde que começou o seu turno. E estava quase na hora de fazer a sua ronda de qualquer maneira. O infeliz no telefone parecia que realmente precisava da sua ajuda. E é bom para alguém poder fazer algo de bom para outra pessoa.

A história de Bill

Bill Goodrock linha um objetivo simples, ao qual se apegava desde que tinha 12 anos: aposentar-se com 24 anos, sem nem tocar em um centavo do seu fundo de poupança. Para mostrar ao pai, o todo-poderoso e impiedoso banqueiro, que ele podia ser um sucesso por conta própria.

Faltavam apenas dois anos e estava perfeitamente claro que ele não iria ganhar a sua fortuna nos próximos 24 meses sendo um homem de negócios brilhante, e também não iria conseguir isso como um investidor inteligente. Certa vez pensou em roubar bancos com um revólver, mas isso é coisa de cinema — o custo do risco comparado ao benefício é alto demais. E ficava sonhando com um golpe — roubar um banco eletronicamente.

Da última vez que Bill esteve na Europa com a família, ele abriu uma conta bancária em Mônaco com Fr$ 100. Ele ainda tinha apenas Fr$ 100 na conta, mas tinha um plano que o ajudaria a chegar aos sete dígitos em um instante. Com um pouco de sorte talvez até aos oito dígitos.

A namorada de Bill, Annemarie, trabalhava em um grande banco em Boston. Um dia, enquanto a esperava sair de uma reunião de última hora no escritório, ele cedeu à curiosidade e conectou o seu laptop a uma porta Ethernet da sala de reuniões que estava usando. Isso mesmo! Ele estava na rede interna e conectado dentro da rede do banco... atrás do firewall corporativo. Isso lhe deu uma idéia.

Ele juntou seu talento ao de um colega de classe que conhecia uma jovem chamada Júlia, uma brilhante mestre em ciência da computação e candidata a um estágio na Marchand Microsystems. Julia parecia ser uma ótima fonte de informações internas essenciais. Eles disseram a ela que estavam escrevendo um roteiro de um filme e ela realmente acreditou neles. Ela pensou que poderia ser divertido criar uma história com eles e deu-lhes todos os detalhes sobre como você poderia executar o plano que haviam descrito. Ela pensou que a idéia era brilhante, e ficava pedindo que eles lhe dessem um crédito no filme também.

Eles a avisaram que com freqüência as idéias para um filme são roubadas e fizeram com que ela jurasse que nunca diria nada a ninguém.

Adequadamente instruídos por Julia, Bill fez ele mesmo a parte mais arriscada e nunca duvidou que conseguiria.

Liguei à tarde e consegui descobrir que o supervisor da noite da força de segurança era um homem chamado Isaiah Adams. Às 21 h30 daquela noite liguei para o prédio e falei com o guarda da segurança da recepção. A minha história baseava-se toda na urgência e eu parecia estar meio em pânico. "Estou com um problema no carro e não consigo chegar até aí", eu disse, "Tenho uma emergência e realmente preciso da sua ajuda. Tentei ligar para o supervisor de segurança, Isaiah, mas ele não está em casa. Você pode me fazer este favor só esta vez? Eu ficaria muito grato!".

As salas daquele prédio enorme tinham códigos de entrada e eu dei-lhe o código do laboratório de computadores e perguntei se ele sabia onde ficava. Ele disse que sim, e concordou em ir até lá para mim. Ele disse que isso levaria alguns minutos e eu respondi que ligaria para ele, dando a desculpa de que estava usando a única linha telefônica disponível e que a estava usando para discar para a rede para tentar resolver o problema.

Ele já estava lá esperando quando liguei e eu lhe expliquei onde encontraria a console na qual eu estava interessado. Ele teria de procurar a console que tinha um banner de papel escrito

"elmer" — o host que Júlia disse que era usado para criar as versões do sistema operacional que a empresa comercializava. Quando ele disse que tinha encontrado, eu soube com certeza que Júlia nos passou boas informações e o meu coração disparou. Pedi para ele dar Enter algumas vezes, e ele comentou que um sinal de libra aparecia. Isso indicava que o computador estava conectado como raiz, a conta de superusuário com todos os privilégios de sistema. Ele não era um bom digitador e foi uma dificuldade fazê-lo digitar o meu próximo comando, o qual era meio complicado mesmo:

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Finalmente ele conseguiu e agora podíamos dar um nome de correção para a conta. Em seguida, fiz com que ele digitasse:

```
echo 'fix::10300:0:0' >> /etc/shadow
```

Isso estabeleceu a senha criptografada, a qual é colocada entre dois pontos duplos. Se não houver nada entre esses dois pontos duplos a conta fica com uma senha nula. Assim sendo, apenas aqueles dois comandos foram necessários para anexar a correção de conta ao arquivo de senhas, com uma senha nula. O melhor de tudo é que a conta teria os mesmos privilégios do superusuário.

A seguir fiz com que ele inserisse um comando de diretório recursivo que imprimia uma longa lista de nomes de arquivo. Depois pedi para ele dobrar o papel, destacar e levá-lo para a sua mesa de segurança porque: "Eu talvez tenha de ler alguma coisa mais tarde."

O mais interessante disso tudo é que ele não tinha a menor idéia de que havia criado uma conta nova. E fiz com que imprimisse a lista de diretório com os nomes de arquivos de que precisava para ter certeza de que os comandos que ele digitou anteriormente sairiam da sala de computadores com ele. Dessa forma, o administrador do sistema ou o operador na manhã seguinte não descobririam nada que os alertasse de que houve uma violação de segurança.

Agora eu tinha uma conta, uma senha e privilégios completos. Um pouco antes da meia-noite disquei e segui as instruções que Júlia havia digitado cuidadosamente "para o filme". Em um piscar de olhos acessei um dos sistemas de desenvolvimento que continha a cópia master do código-fonte da nova versão do sistema operacional da empresa.

Carreguei um *patch* que Júlia havia escrito, o qual, segundo ela, modificava uma rotina em uma das bibliotecas do sistema operacional. O patch, na verdade, criava uma *backdoor* oculta que permitia o acesso remoto ao sistema com uma senha secreta.

Observação

O tipo de backdoor usada aqui não muda o programa de login do sistema operacional em si. Em vez disso, uma função específica contida dentro da biblioteca dinâmica usada pelo programa de login é substituída para criar o ponto de entrada secreto. Nos ataques típicos, os invasores de computador quase sempre substituem ou usam um patch no próprio programa de login, mas os administradores de sistema inteligentes podem detectar a alteração comparando-o com a versão que vem em mídias, tais como um CD-ROM, ou em outros métodos de distribuição.

Jargão

PATCH Tradicionalmente uma parte do código que, quando colocado em um programa executável, corrige um problema.

Segui cuidadosamente as instruções que ela havia escrito para mim, primeiro instalando o patch e, depois, percorrendo as etapas que removiam a correção de conta e limpei todos os registros de auditoria, para que não houvesse rastros das minhas atividades, apagando, assim, as minhas pegadas.

Em breve a empresa começaria a enviar a atualização do novo sistema operacional para seus clientes: as instituições financeiras de todo o mundo. E cada cópia enviada incluiria a backdoor que eu havia colocado na distribuição master antes de ela ser enviada, permitindo que eu acessasse o sistema de computadores de cada banco e corretora que instalasse a atualização.

Obviamente, eu não havia terminado tudo — ainda havia trabalho a fazer. Ainda teria de acessar a rede interna de cada instituição financeira que queria "visitar". Em seguida, teria de descobrir qual computador era usado para as transferências de dinheiro e teria de instalar software de monitoramento para saber quais eram os detalhes de suas operações e exatamente como os fundos eram transferidos.

Tudo isso eu podia fazer à distância em um computador localizado em qualquer lugar. Por exemplo, com a vista de uma praia de areias brancas. Taiti, lá vou eu.

Liguei de volta para o guarda, agradeci sua ajuda e disse que ele poderia rasgar a impressão.

Analisando a trapaça

O guarda de segurança tinha instruções para executar suas tarefas, mas por mais completas que sejam as instruções, não podem prever toda situação possível. Ninguém lhe dissera o dano que poderia ser causado se ele digitasse algumas teclas em um computador para uma pessoa que ele achasse ser um empregado da empresa.

Com a cooperação do guarda ficou relativamente fácil acessar um sistema crítico que armazenava o master de distribuição, apesar do fato de que ele estava trancado em um laboratório seguro. O guarda, obviamente, tinha as chaves de todas as portas trancadas.

Recado do Mitnick

Quando o invasor de computadores não pode ter acesso físico a um sistema de computador ou à própria rede, ele tenta manipular outra pessoa para fazer isso por ele. Nos casos em que o acesso físico é necessário para o plano, o uso da vítima como representante é melhor ainda do que fazer você mesmo, porque o atacante assume menos risco de ser pego e preso.

Até mesmo um empregado honesto (ou, neste caso, a candidata a Ph.D e estagiária da empresa, Júlia) às vezes pode ser enganado para revelar informações de importância crucial para um ataque da engenharia social, tais como onde está localizado o sistema de computadores alvo e — o segredo do sucesso deste ataque — quando eles criariam a nova versão de distribuição do software. Isso é impor-

tante, uma vez que uma mudança desse tipo feita cedo demais tem mais chances de ser detectada ou anulada se o sistema operacional for recriado a partir de um código limpo.

Você observou o detalhe de fazer com que o guarda levasse as folhas impressas de volta para a recepção e as destruísse mais tarde? Essa era uma etapa importante. Quando os operadores de computador chegassem para trabalhar no próximo dia útil, o atacante não queria que eles encontrassem essa evidência no terminal de impressão, nem notassem que estava no lixo. Uma desculpa razoável para que o guarda levasse as folhas evitou esse risco.

O PATCH DE EMERGÊNCIA

Você deve achar que um funcionário do suporte técnico entende os perigos de dar acesso à rede de computadores para um estranho. Mas quando o estranho é um inteligente engenheiro social disfarçado como um útil vendedor de software, os resultados podem não ser aquilo que você espera.

Uma ligação útil

O interlocutor queria saber "Quem é o encarregado dos computadores aí?" e a telefonista o transferiu para o funcionário do suporte técnico, Paul Ahearn.

O interlocutor identificou-se: "Edward, da Seer Ware, o fabricante do seu banco de dados. Aparentemente, vários dos nossos clientes não receberam o e-mail sobre a atualização de emergência. Estamos ligando para alguns para fazer uma verificação do controle de qualidade e saber se houve algum problema com a instalação do patch. Vocês já instalaram a atualização?"

Paul disse que tinha certeza de que não viu nada parecido.

Edward disse: "Bem, isso causaria perdas intermitentes e catastróficas de dados e, portanto, recomendamos que você o instale assim que possível." Paul disse que isso era algo que ele certamente faria. "Muito bem", respondeu o interlocutor. "Podemos enviar um CD com o patch e quero lhe dizer que isso é realmente crítico — duas empresas já perderam diversos dias de dados. Assim sendo, você *realmente* deve instalar esse patch assim que ele chegar, antes que isso aconteça na sua empresa também."

"Não posso fazer o download do seu site Web?", Paul perguntou.

"Ele deve estar disponível em breve — a equipe técnica está apagando todos esses incêndios. Se você quiser, posso ver se o nosso centro de suporte ao cliente o instala remotamente para você. Podemos discar ou usar a Telnet para a conexão com o sistema, se o seu sistema suportar isso."

"Não permitimos a Telnet, particularmente da Internet — ela não é segura", respondeu Paul. "Se você pudesse usar o SSH (Shell seguro) seria bom", ele disse, citando um produto que fornece transferências seguras de arquivo.

"Sim. Temos o SSH. Então qual é o endereço IP?"

Paul deu o endereço IP e quando Edward pediu "e qual é o nome de usuário e senha que posso usar". Paul também forneceu essas informações.

Analisando a trapaça

Obviamente, aquela ligação telefônica poderia realmente ter vindo do fabricante do banco de dados. Mas nesse caso a história não pertenceria a este livro.

O engenheiro social aqui influenciou a vítima criando a sensação assustadora de que poderia haver perda de dados e ofereceu uma solução imediata que resolveria o problema.

Da mesma forma, quando um engenheiro social tem como alvo alguém que sabe o valor das informações, ele precisa ter argumentos muito convincentes e persuasivos para conseguir o acesso remoto. Eventualmente ele precisa incluir o elemento da urgência, para que a vítima se distraia com a pressa e concorde antes de ter uma chance de pensar muito na solicitação.

A NOVA GAROTA

Quais tipos de informações que estão nos arquivos da sua empresa a que um atacante pode ter acesso? As vezes essas informações podem ser algo que você não achava que precisasse proteger.

A ligação para Sarah

"Recursos Humanos, aqui é Sarah."

"Oi Sarah. Aqui é George do estacionamento. Você sabe o cartão de acesso usado para entrar no estacionamento e nos elevadores? Bem, tivemos um problema e precisamos reprogramar os cartões de todos os funcionários novos que foram contratados nos últimos 15 dias."

"Você precisa dos nomes?"

"E dos números de telefone."

"Posso verificar a nossa lista de novos contratados e ligar de volta. Qual é o número do seu telefone?"

"É 73... Ah, estou saindo para o café, que tal se eu ligar de volta em meia hora?"

Tudo bem."

Quando ele ligou de volta, ela explicou: "Ah, sim. Bem, há apenas dois. Anna Myrtle do Financeiro, ela é secretária. E aquele vice-presidente novo, o Sr. Underwood."

"E os números dos telefones?"

"Certo... O número do Sr. Underwood é 6973. O de Anna Myrtle é 2127."

"Olhe, você me ajudou muito. Obrigado."

A ligação para Anna

"Financeiro, Anna."

"Ainda bem que encontrei alguém trabalhando até mais tarde. Aqui é Ron Vittaro, sou editor da divisão de negócios. Acho que ainda não fomos apresentados. Bem-vinda à empresa."

"Obrigada."

"Anna, estou em Los Angeles e em meio a uma crise. Preciso de dez minutos do seu tempo."

"É claro. Do que você precisa?"

"Vá até o meu escritório. Você sabe onde é o meu escritório?"

"Não."

"Muito bem, ele é o escritório de canto do 15°. andar — sala 1502. Vou ligar para lá em alguns minutos. Quando chegar lá, você terá de apertar o botão forward do telefone para que a minha ligação não entre diretamente no meu voice mail."

Tudo bem, estou indo para lá agora."

Dez minutos depois ela estava no escritório, havia cancelado o encaminhamento de chamadas e estava aguardando o telefone tocar. Ele disse para ela sentar-se ao computador e abrir o Internet Explorer. Depois pediu para ela digitar um endereço: www.geocities.com/ron_insen/manuscrípt.doc.exe.

Uma caixa de diálogo apareceu e ele pediu para ela clicar em Open. O computador parecia estar descarregando o manuscrito e, em seguida, a tela ficou em branco. Quando ela disse que algo parecia estar errado, ele respondeu "Ah, *não.* Não de novo. Tenho tido problemas para fazer o download desse site Web com freqüência, mas achei que isso já estivesse resolvido. Muito bem, não se preocupe, vou conseguir esse arquivo de outra maneira mais tarde." Em seguida, ele pediu que ela reinicializasse o seu computador para que ele pudesse ter certeza de que ele inicializaria corretamente após o problema que ela acabou de ter. Ele a orientou sobre como fazer a reinicialização.

Quando o computador estava sendo novamente executado, ele agradeceu muito e desligou. Anna voltou ao departamento financeiro para terminar o trabalho que estava fazendo.

A história de Kurt Dillon

A Millard-Fenton Publishers estava entusiasmada com o novo autor que haviam acabado de contratar, o CEO aposentado de uma empresa da *Fortune 500* que tinha uma história fascinante para contar. Alguém havia passado o homem para um gerente de negócios para concluir as negociações. O gerente de negócios não queria admitir que não sabia nada sobre contratos de publicação e contratou um velho amigo para ajudá-lo a descobrir o que ele precisava saber. O velho amigo, infelizmente, não foi uma boa opção. Kurt Dillon usava aquilo que poderíamos chamar de métodos incomuns de pesquisa, ou seja, métodos que não são totalmente éticos.

Kurt criou um site grátis no Geocities em nome de Ron Vittaro e carregou um programa *spyware* no site novo. Ele mudou o nome do programa para manuscript.doc.exe, para que o nome parecesse ser um documento do Word e não levantasse suspeitas. Na verdade, isso funcionou melhor ainda do que Kurt previra. Como o Vittaro real nunca havia mudado nenhuma das configurações default "Hide file extensions for known file types" do seu sistema operacional Windows, o arquivo era exibido com o nome manuscript.doc.

Jargão

SPYWARE Software especializado usado para monitorar de modo oculto as atividades do computador de um alvo. Um dos meios mais comuns dessa prática é usada para controlar os sites visitados pelos compradores da Internet para que os anúncios online possam ser adaptados aos seus hábitos de pesquisa na Internet. A outra forma análoga é grampear um telefone, exceto que o dispositivo-alvo é um computador. O software captura as atividades do usuário, incluindo as senhas e teclas digitadas, e-mail, conversas de chat, mensagens instantâneas, todos os sites Web visitados e capturas de tela.

Em seguida, fez com que uma amiga ligasse para a secretária de Vittaro. Seguindo as instruções de Dillon, ela disse: "Sou a assistente executiva de Paul Spadone, presidente da Ultimate Bookstores, em Toronto. O Sr Vittaro conheceu o meu chefe em uma feira de livros há algum tempo e pediu para ele ligar e discutir um projeto que eles fariam juntos, O Sr Spadone viaja muito e pediu que eu descobrisse quando o Sr Vittaro estará no escritório."

Quando as duas terminaram de comparar as agendas, a amiga de Dillon já tinha informações suficientes para fornecer ao atacante uma lista das datas em que o Sr Vittaro estaria no escritório. Isso significava que ele também sabia quando Vittaro *estaria fora* do escritório, Não foi preciso conversar muito para descobrir que a secretária de Vittaro aproveitaria a sua ausência para esquiar um pouco. Por um período de tempo curto, ambos estariam fora do escritório. E isso era perfeito.

No primeiro dia que eles deveriam estar fora, ele fez uma ligação urgente só para ter certeza, e foi informado pela recepcionista que "o Sr Vittaro não está no escritório, nem a sua secretária, Nenhum deles deve voltar hoje, amanhã nem depois de amanhã".

A sua primeira tentativa de enganar um empregado para tomar parte nesse esquema foi bem-sucedida, e ela não pestanejou quando ele pediu ajuda para fazer o download de um "manuscrito", o qual na verdade era um conhecido programa comercial spyware que o atacante havia modificado para uma *instalação silenciosa.* Usando esse método, a instalação não seria detectada pelo software antivírus. Por algum motivo, os fabricantes de antivírus não comercializam produtos que detectam o spyware comercial.

Imediatamente após a jovem ter carregado o software no computador de Vittaro, Kurt voltou ao site Geocities e substituiu o arquivo doc.exe por um manuscrito de livro que ele encontrou na Internet. Caso alguém descobrisse o golpe e voltasse ao site para investigar o que havia acontecido, encontraria o manuscrito de um livro inofensivo, amador e que não podia ser publicado.

Após o programa ter sido instalado e o computador reinicializado, ele foi configurado para se tornar imediatamente ativo. Ron Vittaro retornaria à cidade em alguns dias, começaria a trabalhar e o spyware começaria a encaminhar todas as teclas digitadas no seu computador, incluindo os e-mails enviados e as capturas de telas, mostrando o que estava sendo exibido na tela naquele momento. Tudo isso seria enviado a intervalos regulares para um provedor de serviços de e-mail grátis na Ucrânia.

Alguns dias após o retorno de Vittaro, Kurt estava olhando os arquivos de registro da sua caixa de correio ucraniana e em pouco tempo localizou os e-mails confidenciais que indicavam até onde a Millard-Fenton Publishing estava disposta a fazer um acordo com o autor. Munido desse conhecimento, o agente do autor podia negociar mais facilmente termos muito melhores do que aqueles que foram oferecidos originalmente, sem nem correr o risco de perder o acordo totalmente. E isso, é claro, significava uma comissão maior para o agente,

Analisando a trapaça

Neste golpe, o atacante tornou mais provável o seu sucesso escolhendo um empregado novo que agiria como um representante, contando que ela estaria mais disposta a cooperar e fazer parte da equipe e que teria menos chances de conhecer a empresa, o seu pessoal e as boas práticas da segurança, o que poderia atrapalhar a tentativa.

Como Kurt estava usando o nome de um vice-presidente em suas conversas com Anna, que era uma funcionária do departamento financeiro, ele sabia que era pouco provável que ela questionasse a sua autoridade. Ao contrário, ela podia pensar que, ajudando um vice-presidente, tivesse alguma vantagem.

Jargão

INSTALAÇÃO SILENCIOSA **Um método de instalar um aplicativo de software sem que o usuário ou operador do computador tenha conhecimento de que a ação está** ocorrendo,

E o processo pelo qual Anna passou para instalar o spyware parecia ser inofensivo. Anna não linha a menor idéia de que suas ações aparentemente inocentes permitiam que um atacante tivesse informações valiosas que poderiam ser usadas contra os interesses da empresa.

E por que ele escolheu encaminhar a mensagem do vice-presidente para uma conta de e-mail na Ucrânia? Por diversos motivos: um destino distante torna bem menos provável o rastreio ou alguma ação contra um atacante. Esses tipos de crimes geralmente são considerados crimes de baixa prioridade em países com esses, nos quais a polícia tende a fazer vistas grossas para um crime cometido pela Internet, uma vez que essa não é uma ofensa muito séria. Por esse motivo, o uso de e-mails de países que talvez não cooperariam com a aplicação das leis dos EUA é uma estratégia atraente.

EVITANDO A TRAPAÇA

Um engenheiro social sempre prefere visar um empregado que não pode reconhecer algo suspeito em suas solicitações. Isso não apenas facilita o trabalho, mas também o torna menos arriscado — como ilustram as histórias deste capítulo.

Recado do Mitnick

É prática comum pedir que um colega ou subordinado faça um favor. Os engenheiros sociais sabem como explorar o desejo natural das pessoas de ajudar e fazer parte de uma equipe. Um atacante explora esse traço humano positivo para enganar empregados desavisados para que executem ações que o coloquem mais perto do seu objetivo. É importante entender esse conceito simples para que você reconheça quando outra pessoa está tentando manipulá-lo.

Enganando os desavisados

Já enfatizei antes a necessidade de treinar bem os empregados para que nunca se deixem enganar pelas instruções de um estranho. Todos os empregados também precisam entender o perigo de atender uma solicitação para executar qualquer ação no computador de outra pessoa. A política da empresa deve proibir isso, exceto quando for aprovado especificamente por um gerente. As situações permitidas incluem:

- Quando a solicitação for feita por uma pessoa bem conhecida, com a requisição feita frente a frente ou pelo telefone, quando você pode reconhecer sem dúvidas a voz do interlocutor.
- Quando você verifica positivamente a identidade do solicitante por meio de procedimentos aprovados.

- Quando a ação é autorizada por um supervisor ou outra pessoa com autoridade que o solicitante conhece pessoalmente.

Os empregados devem ser treinados para não ajudar pessoas que não conhecem pessoalmente, mesmo que a pessoa alegue ser um executivo. Após a execução das políticas de segurança relativas à verificação, o gerenciamento deve dar suporte aos empregados que seguem essas políticas, mesmo que isso signifique desafiar um membro da equipe executiva que está pedindo para o empregado desrespeitar uma política de segurança.

Cada empresa também precisa ter políticas e procedimentos que orientem os empregados para responder às solicitações para executar alguma ação com computadores ou equipamento relacionado com computador. Na história sobre a editora, o engenheiro social visava um empregado novo que não havia sido treinado nas políticas e procedimentos de segurança da informação. Para evitar esse tipo de ataque, cada empregado novo ou experiente deve ser instruído para seguir uma regra simples. Não usar nenhum sistema de computador para executar uma ação solicitada por um estranho.

Lembre-se de que todo empregado que tenha acesso físico ou eletrônico a um computador ou componente de um equipamento relacionado com computador está sujeito a ser manipulado para executar alguma ação maliciosa por parte de um atacante.

Os empregados, e particularmente o pessoal de TI, precisam entender que permitir o acesso de um estranho às suas redes de computadores é como dar o número da sua conta bancária para um operador de telemarketing ou como dar o seu cartão com o número de telefone para um estranho que está na cadeia. Os empregados devem prestar muita atenção ao fato de a execução de uma solicitação levar à divulgação de informações confidenciais ou comprometer o sistema corporativo de computadores.

O pessoal de TI também deve estar prevenido contra interlocutores desconhecidos que se fazem passar por fornecedores. Em geral, uma empresa deve pensar em ter pessoas específicas designadas como contatos para cada fornecedor de tecnologia, com uma política que diga que outros empregados não responderão às solicitações dos fornecedores que pedem informações ou alterações em qualquer equipamento telefônico ou de computador. Dessa forma, o pessoal designado torna-se conhecido do pessoal do fabricante que ligar ou fizer uma visita e tem menos chance de ser enganado por um impostor. Se um fornecedor ligar mesmo quando a empresa não tiver um contrato de suporte, isso deve levantar suspeita.

Todos os que trabalham na organização precisam ter conhecimento das ameaças e vulnerabilidades da segurança da informação. Observe que os guardas de segurança e outros precisam receber o treinamento não apenas em segurança, mas também na segurança da *informação.* Como os guardas de segurança com freqüência têm acesso físico a toda a instalação, eles devem poder reconhecer os tipos de ataques da engenharia social que podem ser usados contra eles.

Cuidado com o Spyware

O spyware comercial era muito usado pelos pais para monitorar aquilo que seus filhos estavam fazendo na Internet e também pelos empregadores, supostamente para determinar quais empregados estavam deixando de trabalhar para surfar na Internet. Um uso mais sério era para detectar o roubo potencial de ativos de informações ou espionagem industrial. Os desenvolvedores comercializam o seu spyware oferecendo-o como uma ferramenta para proteger as crianças, quando, na verdade, o seu verdadeiro mercado são as pessoas que querem espionar alguém. Hoje em dia, a venda do spyware é motivada

em grande parte pelo desejo das pessoas de saberem se o cônjuge ou outra pessoa importante as está enganando.

Logo depois que comecei a escrever a história sobre o spyware deste livro, a pessoa que recebe e-mails para mim (porque não posso usar a Internet) encontrou uma mensagem de e-mail de spam anunciando um grupo de produtos spyware. Um dos itens oferecido era descrito desta maneira:

> **FAVORITO! OBRIGATÓRIO:** Este poderoso programa de monitoramento e espionagem captura secretamente todas as teclas, a hora e o título de todas as janelas ativas em um arquivo de texto, enquanto é executado oculto no segundo plano. Os registros podem ser criptografados e enviados automaticamente para um endereço de e-mail especificado ou simplesmente gravados no disco rígido. O acesso ao programa é protegido por senha e pode ser oculto do menu CTRL+ALT+DEL
>
> Use-o para monitorar os URLs digitados, as sessões de chat, os e-mails e muitas outras coisas (até mesmo senhas ;-)).
>
> Instale sem detecção um ANY PC e mande os logs para você mesmo por e-mail!!!!!!

Falha do antivírus?

O software antivírus não detecta o spyware comercial, tratando assim o software como não malicioso mesmo que a intenção seja espionar outra pessoa. Assim sendo, o equivalente para computador, os grampos de telefone, não podem ser percebidos e criam riscos que cada um de nós possa estar sendo ilegalmente monitorado a qualquer momento. Obviamente, os fabricantes de software antivírus podem argumentar que o spyware pode ser usado para finalidades legítimas e. portanto, não deve ser tratado como malicioso. Mas determinadas ferramentas que já foram usadas pela comunidade dos hackers, as quais agora são distribuídas ou vendidas livremente como software relacionado com segurança, são tratadas como código malicioso. Existem dois padrões aqui, e eu continuo me perguntando por quê.

Outro item que é oferecido no mesmo e-mail prometia capturar telas do computador do usuário, como se houvesse uma câmera de vídeo olhando por cima dos seus ombros. Alguns desses produtos de software nem exigem o acesso físico ao computador da vítima. Basta instalar e configurar o aplicativo remotamente e você tem um grampo instantâneo de computador! O FBI deve amar essa tecnologia.

Com o spyware disponível tão facilmente, a sua empresa precisa estabelecer dois níveis de proteção. Você deve instalar o software de detecção do spyware tal como o SpyCop (disponível em www.spycop.com) em todas as estações de trabalho e deve exigir que os empregados iniciem varreduras periódicas. Além disso, você deve treinar os empregados contra o perigo de eles serem enganados para fazer o download de um programa ou abrir um anexo de e-mail que pode instalar o software malicioso.

Além de evitar que o spyware seja instalado enquanto um empregado está fora da sua mesa tomando um café, almoçando ou em uma reunião, uma política que obrigue todos os empregados a trancar seus sistemas de computadores com uma proteção de tela com senha ou com um método semelhante diminuiria substancialmente o risco de que uma pessoa não autorizada pudesse acessar o computador de um funcionário. Ninguém que entrasse na sala ou no escritório da pessoa poderia

acessar nenhum dos seus arquivos, ler seus e-mails ou instalar spyware ou outro software malicioso. Os recursos necessários para ativar proteção de tela com senha são nulos e o beneficio de proteger as estações de trabalho dos empregados é substancial. A análise do custo/beneficio nessa circunstância não deve dar trabalho nenhum.

Capítulo 13

Trapaças Inteligentes

Agora você já deve ter desconfiado que quando um estranho liga com uma solicitação de informações confidenciais ou algo que possa ser de valor para um atacante, a pessoa que recebe a ligação deve estar treinada para anotar o número de telefone do interlocutor e ligar de volta para verificar se a pessoa é realmente quem alega ser — um empregado da empresa, um empregado de um parceiro comercial ou um representante do suporte técnico de um dos seus fornecedores. por exemplo.

Mesmo quando uma empresa tem um procedimento estabelecido que deve ser seguido cuidadosamente pelos empregados para verificar as pessoas que estão ligando para a empresa, os atacantes sofisticados ainda podem usar vários truques para enganar suas vítimas e fazer com que elas acreditem que são quem alegam ser. Mesmo os empregados conscientes quanto à segurança podem ser enganados por métodos tais como os descritos a seguir.

O ID ENGANOSO

Todos os que já receberam uma ligação em um telefone celular já observaram o recurso conhecido como identificador de chamadas — aquela exibição conhecida do número do telefone de quem está ligando. Em um ambiente de negócios, esse recurso oferece a vantagem de permitir que um funcionário saiba rapidamente se a ligação vem de um colega ou de fora da empresa.

Há muitos anos alguns phreakers ambiciosos apresentaram-se às maravilhas do ID de chamadas antes que a empresa de telefonia tivesse permissão de oferecer o serviço para o público. Eles se divertiam muito enganando as pessoas ao atender ao telefone e dizer o nome da pessoa que ligou antes mesmo de elas dizerem uma palavra.

Quando você começa a achar que a prática de verificar a identidade, confiando naquilo que vê. é segura — como o que aparece como o ID de chamadas —, você descobre que é exatamente isso que o atacante está querendo.

A ligação telefônica de Linda

Dia/Hora: terça-feira, 23 de julho. I2h00.

Local: os escritórios do Departamento Financeiro da Starbeat Aviation

O telefone de Linda Hill tocou bem quando ela estava escrevendo um memorando para o seu chefe. Ela olhou o ID de chamadas, o qual mostrava que a ligação vinha do escritório corporativo de Nova York. mas de alguém chamado Victor Martin — e não reconheceu esse nome.

Ela pensou em deixar a ligação na secretária eletrônica para não interromper o raciocínio naquele momento. Mas a curiosidade foi maior Ela atendeu ao telefone e o interlocutor apresentou-se e disse que era do Departamento de Recursos e Projetos e estava trabalhando com um material para o CEO, "Ele está a caminho de Boston para reuniões com alguns dos nossos banqueiros. Ele precisa dos principais dados financeiros do trimestre atual", ele explicou. "E mais uma coisa. Ele também precisa das projeções financeiras do projeto Apache," Victor acrescentou usando o nome de código de um produto que seria um dos principais lançamentos da empresa naquele ano,

Ela pediu o seu endereço de e-mail, mas ele respondeu que estava com problemas para receber e-mails e, como o suporte técnico ainda estava tentando solucionar o problema, ele pediu se ela não poderia mandar as informações por fax. Ela disse que sim, e ele deu o ramal interno do seu aparelho de fax,

Ela enviou o fax alguns minutos mais tarde,

Mas Victor não trabalhava no departamento de RP. Na verdade, ele nem trabalhava na empresa.

A história de Jack

Jack Dawkins havia iniciado a sua carreira profissional cedo como um batedor de carteiras nos jogos do Yankee Stadium, nas plataformas superlotadas do metrô e entre os turistas noturnos de Times Square. Ele era tão ágil e habilidoso que podia tirar o relógio do pulso de um homem sem que ele notasse. Mas como todo adolescente, ficou desajeitado e acabou sendo pego. Na prisão para jovens, ele aprendeu uma nova forma de contravenção, a qual representava um risco bem menor de ser pego.

Seu trabalho era obter o demonstrativo trimestral de lucros e perdas da empresa e as informações de fluxo de caixa antes que esses dados fossem arquivados na Comissão de Valores Mobiliários e Câmbio (SEC) e publicados. O seu cliente era um dentista que não queria explicar o motivo pelo qual desejava as informações. Para Jack a precaução daquele homem era uma piada. Ele já conhecia a história — o cliente provavelmente tinha um problema de jogo ou então uma linda e cara namorada da qual a sua mulher ainda não tinha conhecimento. Ou talvez ele apenas tivesse dito à mulher que era muito inteligente ao jogar na bolsa, e agora havia perdido muito e queria fazer um grande investimento em uma coisa certa sabendo se o preço da ação da empresa subiria quando eles anunciassem seus resultados trimestrais.

As pessoas se surpreendem quando descobrem como é rápido para um engenheiro social inteligente descobrir um modo de lidar com uma situação que nunca enfrentou antes. Quando Jack voltou para casa da sua reunião com o dentista, já tinha um plano montado. O seu amigo Charles Bates trabalhava em uma empresa, a Panda Importing, a qual tinha o seu próprio PBX.

Em termos familiares para as pessoas que conhecem os sistemas de telefonia, o PBX estava conectado a um serviço de telefonia digital conhecido como TI. o qual estava configurado como Primary Rate Interface ISDN (integrated services digital network) ou PRI ISDN. Isso significava que sempre que uma ligação era feita da Panda, as informações de configuração e outras informações de processamento passavam por um canal de dados para a central de telefonia da empresa. As informações incluíam o número de quem estava ligando, o qual (a menos que estivesse bloqueado) era entregue no dispositivo de ID de chamadas do receptor.

O amigo de Jack sabia como programar a central para que a pessoa que recebesse a ligação visse em seu ID de chamadas, não o número real de telefone do escritório da Panda, mas sim o número de telefone que ele havia programado na central. Esse truque funciona porque as empresas locais de telefonia não validam o número da ligação recebida do cliente com relação ao número do telefone real pelo qual o cliente está pagando.

Tudo o que Jack Dawkins precisava fazer era acessar qualquer um desses serviços de telefonia. O seu amigo e às vezes parceiro de crimes, Charles Bates, estava sempre disposto a prestar ajuda por uma taxa nominal. Nessa ocasião, Jack e Charles reprogramaram temporariamente a central de telefones da empresa para que as ligações de uma determinada linha de telefone localizada nas instalações da Panda mostrasse o número do telefone interno de Victor Martin, fazendo com que a ligação parecesse vir de dentro da Starbeat Aviation.

A idéia de que o seu ID de chamadas pode mostrar o número que você quiser é tão pouco conhecida que raramente é questionada. Neste caso Linda ficou satisfeita em poder enviar as informações solicitadas por fax para o funcionário que ela achava que era de RP.

Quando Jack desligou. Charles reprogramou a central de telefone da sua empresa e restaurou o número de telefone com as configurações originais.

Analisando a trapaça

Algumas empresas não querem que clientes ou fornecedores saibam os números de telefone de seus empregados. Por exemplo, a Ford pode resolver que as ligações feitas do seu Centro de Suporte ao Cliente mostrem o número 800 do Centro e um nome como "Suporte da Ford", em vez do número real e direto de cada representante do suporte que faz uma ligação. A Microsoft pode dar aos seus empregados a opção de oferecer às pessoas o seu número de telefone em vez de deixar que todos para quem eles ligam possam olhar seu ID de chamadas e saber qual é o seu ramal. Dessa forma, a empresa pode manter a confidencialidade dos números internos.

Mas essa mesma capacidade de reprogramação fornece uma tática útil para o brincalhão, o cobrador, o operador de telemarketing e, obviamente, para o engenheiro social.

VARIAÇÃO: O PRESIDENTE DOS ESTADOS UNIDOS ESTÁ LIGANDO

Como co-patrocinador de um programa de rádio em Los Angeles chamado "O lado negro da Internet" na KFI Talk Radio, trabalhei sob a supervisão do diretor de programação da estação. David era uma das pessoas mais ocupadas e trabalhadoras que já conheci. É muito difícil falar com ele pelo telefone porque ele está sempre ocupado. Ele é uma daquelas pessoas que não responde uma ligação, a menos que veja pelo ID de chamadas que é uma pessoa com quem ele precisa falar.

Como tenho bloqueio de chamadas no meu celular, ele não sabia quem estava ligando e não atendeu a ligação. A ligação foi para a caixa postal e isso foi muito frustrante para mim.

Conversei sobre o que fazer sobre isso com um velho amigo que é co-fundador de uma empresa imobiliária que fornece espaço de escritório para empresas de alta tecnologia. Juntos criamos um plano. Ele tinha acesso à central de telefones Meridian da sua empresa, o que lhe dava a capacidade de programar o número da chamada, como foi descrito na história anterior. Sempre que precisava falar com o diretor de programação e não conseguia, eu pedia que o meu amigo programasse um número que eu escolhia para aparecer no ID de chamadas. Às vezes pedia para ele fazer com que a ligação parecesse vir do escritório da assistente de David, ou talvez da empresa proprietária da estação.

O meu número preferido era o telefone da casa de David, o qual ele atendia sempre. Entretanto. preciso dar um crédito a ele, que sempre tinha um ótimo senso de humor quando atendia ao telefone

e descobria que eu o havia enganado mais uma vez. A melhor parte era que ele ficava na linha o suficiente para descobrir o que eu queria e resolvia o assunto.

Quando demonstrei esse pequeno truque no Art Bell Show, fiz com que o meu ID de chamadas exibisse o nome e o número da sede em Los Angeles do FBI. Art ficou chocado com toda a coisa e me advertiu que eu não poderia fazer algo ilegal. Mas eu disse que isso era perfeitamente legal, desde que não tentasse cometer nenhuma fraude. Após o programa, recebi várias centenas de e-mails pedindo para explicar como eu o havia feito. Agora você vai saber.

Esta é a ferramenta perfeita para criar credibilidade para o engenheiro social. Se, por exemplo, durante o estágio de pesquisa do ciclo de ataques da engenharia social, for descoberto que o alvo tem um ID de chamadas, o atacante pode colocar seu próprio número como sendo de uma empresa ou empregado de confiança. Um cobrador pode fazer com que a sua ligação venha do seu local de trabalho.

Mas pare e pense sobre as implicações disso. Um invasor de computador pode ligar para sua casa alegando ser do departamento de TI da sua empresa. A pessoa que ligou precisa urgentemente da sua senha para restaurar os arquivos de um servidor em pane. O ID de chamadas também pode exibir o nome e o número do seu banco ou corretora, a garota de voz bonita parece precisar apenas verificar os seus números de conta e o nome de solteira da sua mãe. Como medida de segurança, ela também precisa verificar o seu código de caixa eletrônico por causa de algum problema no sistema. Uma telefonista da sala da bolsa de valores pode fazer com que suas ligações pareçam vir da Merrill Lynch ou do Citibank. Alguém que quer roubar a sua identidade pode ligar, aparentemente da Visa, e convencê-lo a lhe dar o seu número do cartão Visa. Um cara rancoroso pode ligar e dizer ser da Receita Federal ou da Polícia Federal.

Se você tiver acesso a um sistema de telefones conectado a um PRI e mais um pouco de conhecimento de programação que provavelmente pode adquirir no site Web do fabricante do sistema, você pode usar essa tática para planejar truques legais para aplicar nos seus amigos. Você conhece alguém com ambiciosas aspirações políticas? Você pode programar o número como 202 456-1414, e seu ID de ligação exibirá o nome "CASA BRANCA".

Ele vai pensar que está recebendo uma ligação do presidente!

A moral da história é simples: não confie no ID de chamadas, exceto quando ele for usado para identificar ligações internas. Tanto em casa quanto no trabalho, todos precisam ter consciência desse truque e reconhecer que o nome ou o número de telefone mostrado em um ID de chamadas não pode ser usado como uma verificação de identidade confiável.

Recado do Mitnick

Da próxima vez que você receber uma ligação e o ID mostrar que ela vem da mamãe, não confie — ela pode estar vindo de um amável engenheiro social.

O EMPREGADO INVISÍVEL

Shirley Cutlass encontrou uma nova e interessante forma de ganhar dinheiro rápido. Não é mais preciso trabalhar duro nas minas de sal. Ela se juntou a centenas de outros artistas do golpe envolvidos no crime da década. Ela é uma ladra de identidades.

Hoje ela voltou a sua atenção para a obtenção de informações confidenciais do departamento de serviço ao cliente de uma administradora de cartões de crédito. Após fazer a lição de casa normal. ela liga para a empresa-alvo e diz para o operador que atende que gostaria de ser transferida para o Departamento de Telecomunicações. Quando a ligação é completada, ela pede para falar com o administrador da caixa postal.

Usando as informações coletadas na sua pesquisa, ela explica que o seu nome *é* Norma Todd e que trabalha no escritório em Cleveland. Usando um truque que agora já deve ser familiar para você. ela diz que vai viajar para a sede corporativa por uma semana, e vai precisar de uma caixa postal lá para que não tenha de fazer ligações interurbanas para verificar suas mensagens. Ela nem precisa de uma conexão de telefone física, uma caixa postal de voice mail basta. Ele diz que vai cuidar disso e que liga depois quando estiver pronto com as informações que ela vai precisar.

Com voz sedutora, ela explica: "Estou a caminho de uma reunião, posso ligar de volta em uma hora?"

Quando ela liga de volta, ele conta que está tudo pronto e fornece as informações — o número do ramal e a senha temporária. Ele pergunta se ela sabe como mudar a senha da caixa postal e ela deixa que ele a ensine, embora saiba tão bem quanto ele.

"E por falar nisso", ela pergunta, "qual número eu disco do meu hotel para verificar minhas mensagens?". Ele lhe dá o número.

Shirley telefona, muda a senha e grava a sua nova mensagem.

Shirley ataca

Até agora foi tudo fácil. Ela já está pronta para usar a arte da fraude.

Ela liga para o departamento de serviço ao cliente da empresa. "Sou da Cobrança do escritório de Cleveland", ela afirma, e inicia uma variação da conhecida desculpa "o meu computador está sendo consertado pelo suporte técnico e preciso da sua ajuda para procurar algumas informações". Ela fornece o nome e a data de nascimento da pessoa cuja identidade ela pretende roubar. Em seguida. relaciona as informações que quer: o endereço, o nome de solteira da mãe, o número do cartão, o limite de credito, o saldo disponível e o histórico de pagamentos. "Ligue de volta para mim neste número", ela diz, e dá o número do ramal interno que o administrador da caixa postal criou para ela. "E se eu não estiver disponível, por favor deixe as informações na minha caixa postal."

Ela se mantém ocupada no restante da manhã e, em seguida, verifica a sua caixa postal à tarde. Está tudo lá, tudo que pediu. Antes de desligar, Shirley limpa a mensagem; não seria cuidadoso deixar para trás uma gravação da sua voz.

E o roubo de identidade, o crime de maior crescimento da América, o crime "in" do novo século, está para fazer outra vitima. Shirley usa as informações de identidade e do cartão de crédito que acabou de obter e começa a fazer compras no cartão da vítima.

Analisando a trapaça

Neste golpe o atacante primeiro enganou o administrador de caixa postal da empresa para que ele acreditasse que ela era uma funcionária e criasse uma caixa postal temporária. Se ele se desse ao trabalho de fazer uma verificação, teria descoberto que o nome e o número de telefone que ela deu coincidiam com as listagens do banco de dados de funcionários da corporação.

O restante era apenas uma questão de dar uma desculpa razoável sobre um problema no computador, pedir as informações desejadas e solicitar que a resposta fosse deixada na caixa postal. E por que algum empregado relutaria em compartilhar das informações com um colega? Como o número de telefone que Shirley deu era, sem dúvida, um ramal interno, não havia motivo para nenhuma suspeita.

Recado do Mitnick

Tente ligar para a sua própria caixa postal de vez em quando. Se ouvir uma mensagem que não é a sua, você pode ter acabado de encontrar o seu primeiro engenheiro social.

A SECRETARIA ATENCIOSA

Cracker Robert Jorday invadia regularmente as redes de computadores de uma empresa global, a Rudolfo Shipping, Inc. A empresa por fim reconheceu que alguém estava atacando o seu servidor de terminais e que por meio daquele servidor o usuário poderia se conectar a qualquer sistema de computadores da empresa. Para salvaguardar a rede corporativa, a empresa resolveu exigir uma senha de discagem em cada servidor de terminal.

Robert ligou para o Centro de Operações de Rede fingindo ser um advogado do departamento Jurídico e disse que estava com problemas para se conectar à rede. O administrador explicou que eles tiveram alguns problemas recentes de segurança e que os usuários de acesso por discagem teriam de obter a senha mensal com seus gerentes. Robert queria saber qual método estava sendo usado para comunicar a senha de cada mês para os gerentes e como ele poderia obtê-la. A resposta foi que a senha do próximo mês seria enviada em um memorando por meio do correio eletrônico do escritório para cada gerente da empresa.

Isso facilitava as coisas. Robert pesquisou um pouco, ligou para a empresa após o primeiro dia do mês e falou com a secretária de um dos gerentes, a qual lhe deu o nome de Janet. Ele disse: "Oi, Janet. Aqui é Randy Goldstein, de Pesquisa e Desenvolvimento. Sei que provavelmente já recebi o memorando com a senha deste mês para a conexão no servidor de terminais de fora da empresa, mas não o estou encontrando. Você já recebeu o seu memorando deste mês?"

Sim, ela disse que já havia recebido.

Recado do Mitnick

O engenheiro social habilidoso é muito inteligente e consegue influenciar as outras pessoas para que elas prestem favores a ele. O recebimento de um fax e o seu encaminhamento para outra localização parece ser tão inofensivo que é fácil convencer uma recepcionista ou outra pessoa a fazer isso. Quando alguém pede um favor envolvendo informações, se você não o conhecer ou não puder verificar a sua identidade, simplesmente diga não.

Ele perguntou se ela poderia enviá-lo por fax para ele e ela concordou. Ele deu o número do fax da recepcionista de um prédio diferente na sede da empresa, e já havia tomado providências para

que os faxes fossem guardados e, em seguida, enviados para ele. Desta vez, porém. Robert usou um método de encaminhamento de fax diferente. Ele deu à recepcionista o número de um fax que caía em um serviço de fax on-line. Quando esse serviço recebe um fax, um sistema automatizado o envia para o endereço de correio eletrônico do assinante.

A nova senha chegou no e-mail que Robert criou em um serviço de correio eletrônico grátis na China. Ele tinha certeza de que se o fax fosse rastreado, o investigador ficaria desesperado tentando ter a cooperação dos oficiais chineses, os quais, como ele sabia, relutavam em ajudar nessas questões. O melhor de tudo é que ele nunca precisou aparecer fisicamente na localização da máquina de fax.

TRIBUNAL DE TRÂNSITO

Provavelmente todos que já tiveram uma multa por excesso de velocidade já sonharam em encontrar uma maneira de não pagá-la. Não indo para a escola de trânsito ou simplesmente tentando convencer o juiz de algum detalhe técnico tal como a velocidade permitida, tempo da notificação da multa, desde que o velocímetro do carro de polícia ou o equipamento de radar não fossem verificados. Não, o cenário mais interessante seria não pagar a multa enganando o sistema.

O golpe

Embora não recomende que você experimente este método de burlar uma multa de trânsito (como se diz. não tente fazer em casa), mesmo assim este é um bom exemplo de como a arte da fraude pode ser usada para ajudar o engenheiro social. Vamos chamar este infrator de trânsito de Paul Durea.

Primeiras etapas

"LAPD, Divisão Hollenbeck."

"Oi, gostaria de falar com o Controle de Intimações."

"Eu sou o atendente de intimações."

"Bom. Aqui é o advogado John Leland, da Meecham, Meecham, and Talbott. Preciso intimar um oficial sobre um caso."

"Muito bem, quem é o oficial?"

"Você tem um Oficial Kendall na sua divisão?"

"Qual é o seu número de série."

"21349."

"Sim. Quando você precisa que ele esteja lá?"

"No próximo mês. mas preciso intimar diversas outras testemunhas do caso e, em seguida, tenho de dizer ao tribunal quais dias serão bons para nós. Existe algum dia no próximo mês em que o Oficial Kendall não estará disponível?"

"Vejamos... Ele tem férias entre os dias 20 e 23 e treinamento nos dias 8 e 16."

"Obrigado. Isso é tudo o que eu preciso agora. Ligo novamente quando a data do julgamento estiver marcada."

Tribunal Municipal, Balcão de Atendimento

Paul: "Gostaria de marcar uma data de julgamento para uma multa de trânsito."

Atendente: "Muito bem. Pode ser no dia 26 do próximo mês?"

"Bem, gostaria de marcar uma apelação."

"Você quer uma apelação para uma multa de trânsito?"

Sim.

"Muito bem. Podemos marcar a apelação para amanhã de manhã ou à tarde. Como você prefere?"

"À tarde."

"A apelação será amanhã, 13h30, na sala de julgamento seis."

"Obrigado, estarei lá."

Tribunal Municipal, Sala de Julgamento Seis

Data: terça-feira, 13h45.

Atendente: "Sr. Durea, por favor, se aproxime."

Juiz: "Sr. Durea, o senhor entende os direitos que lhe foram explicados esta tarde?"

Paul: "Sim, Meritíssimo."

Juiz: "Quer aproveitar a oportunidade e freqüentar a escola de trânsito? O seu caso será fechado após a conclusão de um curso de oito horas. Verifiquei seus registros e o senhor tem esse direito no momento."

Paul: "Não. Meritíssimo. Solicito respeitosamente que o caso seja enviado para julgamento. Mais uma coisa. Meritíssimo. Estarei fora do país, mas estarei disponível nos dias 8 ou 9. Seria possível marcar o meu julgamento em um desses dias? Estou indo para a Europa a negócios amanhã e volto em quatro semanas."

Juiz: 'Muito bem. O julgamento está marcado para 8 de junho às 8h30, sala de julgamento quatro."

Paul: "Obrigado, Meritíssimo,"

Tribunal Municipal, Sala de Julgamento Quatro

Paul chegou cedo no dia 8. Quando o juiz chegou, o atendente deu-lhe uma lista dos casos nos quais os oficiais não apareceram. O juiz chamou os acusados, incluindo Paul, e disse que seus casos estavam encerrados.

Analisando a trapaça

Quando um oficial lavra uma multa, ele a assina com o seu nome e o número do seu crachá (ou o seu número pessoal usado pelo departamento). Encontrar a delegacia é fácil. Uma ligação para o auxílio à lista com o nome do departamento mostrado na citação (patrulha rodoviária, delegacia local ou outro) é suficiente para colocar os pés lá dentro. Após o contato com a agência, eles podem dar o número correto do telefone de um atendente de citações que atende a área geográfica na qual a ocorrência foi feita.

Os policiais são intimados a aparecer em juízo com regularidade, de acordo com o território. Quando um promotor público ou um advogado de defesa precisam que um oficial testemunhe, se ele souber como o sistema funciona, primeiro verifica se o oficial estará disponível. Isso é fácil de fazer; basta uma ligação telefônica para o atendente de intimações daquela agência.

Em geral, nessas conversas o advogado pergunta se o oficial em questão estará disponível em tal data. Para este golpe, Paul precisava ter um pouco de tato. Ele tinha de oferecer um motivo plausível para que o atendente lhe dissesse as datas em que o oficial *não* estaria disponível.

Quando foi ao tribunal pela primeira vez, por que Paul simplesmente não disse ao atendente da corte a data que ele queria? Pelo que entendi, os atendentes do tribunal de trânsito na maior parte dos lugares não permitem que membros do público selecionem as datas de julgamento. Se uma data sugerida pelo atendente não servir para a pessoa, ela tem uma ou duas alternativas, mas isso é o máximo que consegue. Por sua vez, todos que estiverem dispostos a aparecer para uma apelação têm mais chances de ter sorte.

Paul sabia que ele tinha direito a uma apelação. E sabia que os juizes quase sempre estão dispostos a atender uma solicitação de data específica nesses casos. Assim sendo, pediu cuidadosamente as datas que coincidiam com os dias de treinamento do oficial, sabendo que nesse estado o treinamento do oficial tem precedência sobre o comparecimento ao tribunal de trânsito.

Recado do Mitnick

A mente humana é uma criação maravilhosa. É interessante notar como as pessoas podem ser criativas para desenvolver modos fraudulentos de conseguir o que querem ou de se livrarem de uma situação difícil. Você tem de usar a mesma criatividade e imaginação para salvaguardar as informações e os sistemas de computadores dos setores públicos e privados. Assim sendo, pessoal, ao criarem as políticas de segurança da sua empresa, sejam criativos e pensem de forma inovadora.

E, no tribunal de trânsito, quando o oficial não aparece, o caso é encerrado. Sem multas, sem escola de trânsito, sem problemas. E o melhor de tudo é que não fica nenhum registro da infração de trânsito!

Acho que alguns oficiais de policia, oficiais de tribunais, promotores públicos e outros lerão esta história e balançarão a cabeça porque sabem que esse golpe funciona. Mas balançar a cabeça é tudo que podem fazer. Nada vai mudar. Estaria disposto a aceitar uma aposta. Como diz o personagem Cosmo, no filme *Sneakers,* de 1992: "Tudo se resume a uns e zeros" — isso significa que no final tudo se resume às informações.

Enquanto os departamentos de polícia estiverem dispostos a dar informações sobre a escala de um oficial para quase todos que ligarem, a capacidade de se livrar das multas de trânsito continuará existindo. Você tem lacunas semelhantes nos procedimentos da sua empresa ou organização, as quais podem ser usadas por um engenheiro social inteligente para obter as informações que você preferiria que ele não tivesse?

A VINGANÇA DE SAMANTHA

Samantha Gregson estava zangada.

Ela havia trabalhado muito na sua tese de bacharelado em administração e acumulou uma pilha de financiamentos para educação para realizá-la. Ela sempre ouviu falar que uma faculdade era o modo de conseguir uma carreira, em vez de um emprego, e ganhar muito dinheiro. E quando se formou, não conseguiu encontrar um trabalho decente em lugar nenhum.

Ela ficou muito feliz ao receber uma proposta da Lambeck Manufacturing. Certamente, era humilhante aceitar a posição de secretária, mas o Sr. Cartright havia dito que estava ansioso para contratá-la e essa posição de secretária lhe daria a chance de se candidatar para a próxima posição interessante que surgisse.

Dois meses mais tarde ela ficou sabendo que o gerente de produtos júnior de Cartright estava saindo. Ela mal pode dormir naquela noite, imaginando a si mesma no quinto andar em um escritório com porta, participando de reuniões e tomando decisões.

Na manhã seguinte a primeira coisa que fez foi falar com o Sr. Cartright. Ele disse que eles achavam que ela precisava aprender mais sobre a empresa antes de estar pronta para uma posição de gerência. E, em seguida, contrataram um amador de fora que sabia menos sobre a empresa do que ela.

Nessa época ela começou a pensar: a empresa tem muitas mulheres, mas em sua maior parte elas eram todas secretárias. Eles jamais lhe dariam um emprego na administração.

O troco

Levou quase uma semana para ela descobrir como lhes daria o troco. Cerca de um mês antes um rapaz de uma revista especializada havia tentado suborná-la quando veio participar do lançamento do novo produto. Algumas semanas depois, ele ligou para ela no trabalho e disse que lhe enviaria flores se ela lhe desse algumas informações antecipadas sobre o produto Cobra 273, e se essas informações fossem realmente boas e ele as usasse na revista, ele faria uma viagem especial até Chicago para levá-la para jantar.

Um dia depois disso ela havia estado no escritório do Sr. Johannson logo depois de ele ter feito o login na rede corporativa. Sem pensar, ela observou seus dedos *{surfar sobre os ombros,* como também é chamado). Ele havia inserido a senha "marty63".

O seu plano estava começando a tomar forma. Ela se lembrava de ter digitado um memorando não muito tempo depois que entrou na empresa. Encontrou uma cópia nos arquivos e digitou uma nova versão usando a linguagem do memorando original. A sua versão dizia:

> PARA: C. Pania, departamento de TI
>
> DE: L. Cartright, Desenvolvimento
>
> Martin Johannson vai trabalhar com uma equipe de projetos especiais no meu departamento.
>
> Eu o autorizo a ter acesso aos servidores usados pelo grupo de engenharia. O perfil de segurança do Sr. Johannson deve ser atualizado para que ele tenha os mesmos direitos de acesso de um desenvolvedor de produto.
>
> Louis Cartright

Quando a maioria das pessoas saiu para almoçar, ela recortou a assinatura do Sr. Cartright do memorando original e, em seguida, colou-a na sua nova versão e passou corretivo branco nas laterais

Jargão

SURFAR SOBRE OS OMBROS **O ato de observar uma pessoa digitando no teclado do computador para descobrir e roubar sua senha ou outras informações de usuário.**

do papel recortado. Fez uma cópia do resultado e uma cópia da cópia. Mal dava para ver as laterais ao redor da assinatura.

Ela enviou o fax da máquina do escritório do Sr. Cartright.

Três dias depois ela ficou até mais tarde e esperou até que todos fossem embora. Ela foi ao escritório de Johannson e tentou fazer o login na rede com o nome de usuário e a senha marty63. Isso funcionou.

Em minutos ela havia localizado os arquivos de especificação de produto do Cobra 273 e havia feito o seu download para um disco Zip. O disco estava em segurança na sua bolsa enquanto caminhava pela noite fria até o estacionamento. O disco seria enviado para o repórter naquela noite.

Analisando a trapaça

Um empregado zangado, uma pesquisa nos arquivos, uma operação rápida de recortar, colar e passar corretivo, algumas cópias criativas e *voilà* — ela teve acesso às especificações confidenciais de marketing e produto.

E alguns dias depois, um jornalista especializado publica um furo de reportagem com as especificações e os planos de marketing de um novo produto que estará nas mãos dos assinantes da revista e de toda a indústria meses antes do lançamento do produto. As empresas concorrentes terão vários meses para desenvolver produtos equivalentes e criarem suas campanhas publicitárias para derrotar o Cobra 273.

Naturalmente a revista nunca dirá quem lhes deu o furo.

EVITANDO A TRAPAÇA

Quando solicitados a darem informações valiosas, confidenciais ou críticas com as quais um concorrente ou outra pessoa pode se beneficiar, os empregados devem estar cientes de que o uso do ID de chamadas como um meio de verificar a identidade de um interlocutor externo não é um método aceitável. Alguns outros meios de verificação devem ser usados, tais como verificar com o supervisor da pessoa se a solicitação foi apropriada e se o usuário tem autorização para receber as informações.

O processo de verificação requer um ponto de equilíbrio que cada empresa deve definir ela mesma: segurança *versus* produtividade. Qual prioridade será dada à implantação das medidas de segurança? Os empregados resistirão aos procedimentos de segurança e mesmo assim os burlarão para concluir as responsabilidades do seu cargo? Os empregados entendem o motivo pelo qual a segurança é importante para a empresa e para si mesmos? Essas questões precisam ser respondidas para desenvolver uma política de segurança baseada na cultura corporativa e nas necessidades de negócios.

A maioria das pessoas inevitavelmente encara como um aborrecimento tudo aquilo que interfira na sua capacidade de fazer o trabalho e pode burlar todas as medidas de segurança que pareçam ser

uma perda de tempo. A motivação dos empregados para que a segurança faça parte das suas responsabilidades diárias por meio da educação e da conscientização é vital.

Embora o serviço de ID de chamadas nunca deva ser usado como um meio de autenticação das chamadas por voz de fora da empresa, outro método chamado identificação automática de número (AN1) pode ser usado. Esse serviço é fornecido quando uma empresa assina os serviços de ligação grátis em que paga as ligações recebidas e tem direito à identificação. Ao contrário do ID de chamadas, a central da empresa de telefonia não usa nenhuma informação que seja enviada de um cliente quando fornece o número da ligação. O número transmitido pelo AN1 é o número de faturamento designado à parte de quem está ligando.

Observe que diversos fabricantes de modem já incluíram o recurso de ID de chamadas em seus produtos, protegendo as redes corporativas e recebendo apenas as ligações de acesso remoto que estão em uma lista de números de telefone pré-autorizados. Os modems com ID de chamadas são um meio aceito de autenticação em um ambiente de baixa segurança, mas, como já deve ter ficado claro. os invasores de computadores conseguem burlar facilmente o ID de chamadas, e este não deve ser usado para provar a identidade ou a localização de quem liga para um ambiente de alta segurança.

Para abordar o caso de roubo de identidade, como na história sobre como enganar um administrador para que ele crie uma caixa postal de voice mail no sistema de telefones da empresa, crie uma política na qual todo o serviço de telefonia, todas as caixas postais de voice mail e todas as entradas na lista corporativa, tanto impressas quanto on-line, sejam solicitadas por escrito em um formulário fornecido para essa finalidade. O gerente do empregado deve assinar a solicitação e o administrador da caixa postal deve verificar a assinatura.

A política de segurança corporativa deve exigir que as contas de computador novas ou atualizações nos direitos de acesso sejam concedidas apenas após a verificação positiva da pessoa que faz a solicitação, tal como uma ligação para o gerente ou administrador do sistema ou seu representante no número de telefone relacionado no diretório impresso ou on-line da empresa. Se a empresa usar o correio eletrônico seguro no qual os empregados podem assinar digitalmente as mensagens, esse método de verificação alternativo também pode ser aceito.

Lembre-se de que cada empregado, independentemente de ter ou não acesso aos sistemas de computadores da empresa, pode ser enganado por um engenheiro social. Todos devem ser incluídos no treinamento de segurança. Os assistentes administrativos, as recepcionistas, os operadores de telefone e os guardas de segurança devem estar familiarizados com os tipos de ataques da engenharia social que podem sofrer. Dessa forma, eles estarão mais preparados para se defender desses ataques.

Capítulo 14

A Espionagem Industrial

A ameaça de ataques contra as informações do governo, das corporações e dos sistemas universitários é bem conhecida. Quase todos os dias, os meios de comunicação reportam um novo vírus de computador, ataques de navegação de serviço ou uma fraude envolvendo cartões de crédito em um site de comércio eletrônico.

Lemos sobre casos de espionagem industrial, tal como a Borland acusando a Symantec pelo roubo de informações sigilosas, a Cadence Design Systems processando um concorrente pelo roubo do código-fonte de um produto. Muitas pessoas de negócios lêem as histórias e pensam que isso nunca acontecerá com a sua empresa e, na verdade, isso acontece todos os dias.

VARIAÇÃO SOBRE UM MESMO ESQUEMA

O golpe descrito na próxima história provavelmente foi aplicado muitas vezes, embora pareça ser tirado de um filme de Hollywood, como o *O Informante*, ou das páginas de um romance de John Grisham.

Ação de classe

Imagine que uma ação coletiva movida por uma classe esteja assolando uma grande empresa farmacêutica, a Pharmomedic. A ação diz que eles sabiam que uma de suas drogas mais conhecidas tinha um efeito colateral devastador, mas que esse efeito não seria conhecido até que um paciente o tomasse durante vários anos. A ação alega que eles tinham resultados de diversos estudos de pesquisa que revelavam esse perigo, mas que suprimiam a evidência e nunca chegavam ao FDA como deveriam.

William ("Billy") Chaney, o advogado responsável pela ação na empresa de advocacia de Nova York que entrou com a ação coletiva, tem os testemunhos de dois médicos da Pharmomedic que fundamentam a causa. Mas ambos estão aposentados, eles não têm arquivos ou documentação e nenhum deles seria uma testemunha forte e convincente. Billy sabe que está caminhando em areia movediça. A menos que possa conseguir uma cópia de um daqueles relatórios ou de algum memorando interno ou comunicação entre os executivos da empresa, toda a ação será inútil.

Assim sendo, ele contrata uma empresa que já utilizou antes: a Andreeson and Sons, de detetives particulares. Billy não sabe como Pete e o seu pessoal conseguem fazer o que fazem, e nem quer saber Tudo o que sabe é que Pete Andreeson é um bom detetive.

Para a Andreeson, um trabalho como esse é aquilo que chama de um trabalho de caixa preta. A primeira regra utilizada é garantir que os escritórios de advocacia e as empresas que os contratam

nunca saibam como eles obtêm essas informações para sempre negarem tudo de forma plausível. Se alguém vai enfiar os pés em água fervendo, esse alguém será Pete e, pelo que ele recebe pelos grandes trabalhos, ele calcula que o risco compensa. Além disso, ele tem a satisfação pessoal de ser mais inteligente do que as pessoas inteligentes.

Sc os documentos que Chaney quer que ele encontre realmente existiram e não foram destruídos, eles terão de estar em algum lugar dos arquivos da Pharmomedic. Mas encontrá-los em meio aos inúmeros arquivos de uma grande corporação é uma tarefa gigantesca. Por outro lado, suponhamos que eles tenham passado cópias para a sua empresa de advocacia, a Jenkins and Petry. Se os promotores públicos sabiam daqueles documentos e não os apresentaram como parte do processo de descoberta, então eles violaram a ética da profissão e violaram também a lei. Pela cartilha de Pete, isso torna qualquer ataque justo.

O ataque de Pete

Pete faz com que algumas das pessoas que trabalham para ele realizem uma pesquisa e em questão de dias descobre em qual empresa a Jenkins and Petry armazena os seus backups externos. E descobre que a empresa de armazenamento mantém uma lista com os nomes das pessoas autorizadas pela empresa de advocacia a pegarem as fitas do armazenamento. Ele também descobre que cada uma dessas pessoas tem a sua própria senha. Pete envia duas pessoas em uma missão de caixa preta.

Os homens abrem o cadeado usando uma arma para abrir cadeados que pode ser comprada na Web em www.southord.com. Em alguns minutos eles entram nos escritórios da empresa de armazenamento lá pelas 3 horas da manhã e inicializam um PC. Eles sorriem quando vêem o logotipo do Windows 98 porque isso significa que o trabalho será fácil. O Windows 98 não requer nenhuma forma de autenticação. Após um pouco de pesquisa, eles localizam um banco de dados do Microsoft Access com os nomes das pessoas que cada um dos clientes da empresa de armazenamento autorizou para pegar as fitas. Eles incluem um nome falso na lista de autorizações da Jenkins and Petry, um nome igual àquele de uma carteira de motorista falsa que um dos homens já havia conseguido. Eles poderiam ter invadido a área trancada e tentado localizar as fitas que o cliente queria? E claro que sim. Mas, nesse caso, todos os clientes da empresa, incluindo a empresa de advocacia certamente, seriam notificados sobre a invasão. E os atacantes teriam perdido uma vantagem: os profissionais sempre gostam de deixar uma porta aberta para acesso futuro, caso precisem.

Seguindo uma prática-padrão dos espiões industriais de manter algo no bolso do colete para uso futuro, eles também fizeram uma cópia em disquete do arquivo que continha a lista de autorizações. Nenhum deles sabia quando isso poderia ser útil, mas essa era uma das coisas do tipo "Já que estamos aqui, vamos aproveitar", que de vez em quando podem ser aproveitadas.

No dia seguinte, um daqueles mesmos homens ligou para a empresa de armazenamento usando o nome que haviam incluído na lista de autorizações e deu a senha correspondente. Ele pediu todas as fitas da Jenkins and Petry datadas desde o último mês e disse que um serviço de mensageiros passaria lá para pegar o pacote. No meio da tarde, Andreeson tinha as fitas. O seu pessoal restaurou todos os dados para seu próprio sistema de computadores e fez a pesquisa. Andreeson estava muito satisfeito com o fato de a empresa de advocacia, assim como a maioria das outras empresas, não ter se importado em criptografar seus dados de backup.

As fitas foram devolvidas à empresa de armazenamento no dia seguinte e ninguém se deu conta.

Analisando a trapaça

Devido à fraca segurança física, os espiões puderam facilmente abrir o cadeado da empresa de armazenamento, ter acesso ao computador e modificar o banco de dados que continha a lista de pessoas autorizadas a acessar a unidade de armazenamento. A inclusão de um nome à lista permitiu que os impostores obtivessem as fitas de backup de computador que estavam procurando, sem ter de invadir a unidade de armazenamento da empresa. Como a maioria das empresas não criptografa os dados de backup, as informações estavam à sua disposição.

Recado do Mitnick

As informações valiosas devem estar protegidas independente da forma assumida ou do local onde estão armazenadas. A lista de clientes de uma organização tem o mesmo valor seja na forma impressa seja em um arquivo eletrônico no seu escritório ou em um cofre. 05 engenheiros sociais sempre preferem o ponto de ataque mais fácil e menos defendido. As instalações de armazenamento de backup externas a uma empresa são vistas como menos arriscadas. Cada organização que armazena dados valiosos, confidenciais ou críticos com terceiros deve criptografar seus dados para proteger a sua confidencialidade.

Esse incidente fornece mais um exemplo de como uma empresa fornecedora que não toma medidas razoáveis de precaução pode facilitar o comprometimento das informações de seus clientes por parte de um atacante.

O NOVO PARCEIRO DE NEGÓCIOS

Os engenheiros sociais têm uma grande vantagem sobre os golpistas e trapaceiros, e essa vantagem é a distância. Um trapaceiro só pode enganar você se estiver na sua presença, o que permite que depois você dê uma boa descrição dele ou mesmo ligue para a polícia se descobrir o golpe suficientemente cedo.

Os engenheiros sociais evitam esse risco como se ele fosse uma praga. Eventualmente, porém, o risco é necessário e justificado pela boa recompensa.

A história de Jessica

Jessica Andover estava muito feliz porque havia conseguido um emprego em uma empresa de robótica. Esse seria apenas o início e eles não podiam pagar muito, mas a empresa era pequena, as pessoas amistosas e havia a esperança de saber que as suas opções de ação poderiam deixá-la rica. Muito bem, talvez ela não ficasse milionária como os fundadores da empresa, mas mesmo assim ela seria bem rica.

Foi por isso que Rick Daggot tinha um sorriso radiante quando entrou na recepção naquela manhã de terça-feira de agosto. Em seu terno de aparência cara (Armani), usando um pesado relógio de pulso de ouro (um Rolex President) e um impecável corte de cabelo, ele tinha aquele mesmo ar de confiança que deixava todas as garotas loucas quando Jessica estava no colégio.

"Oi", ele disse. "Sou Rick Daggot e estou aqui para uma reunião com Larry."

Jessica sorriu sem graça. "Larry?", ela indagou. "Larry está de férias esta semana."

"Tenho um hora marcada com ele à uma da tarde. Acabei de voar de Louisville para encontrá-lo", disse Rick, tirando o seu Palm e ligando-o para mostrar à ela.

Ela olhou para o Palm e balançou levemente a cabeça. "No dia 20", ela leu. "Isso é na próxima semana." Ele pegou o palmtop de volta e ficou olhando para ele. "Ah, não!", ele resmungou. "Não posso acreditar que cometi um erro assim tão estúpido."

"Posso pelo menos reservar o vôo de volta?", ela perguntou sentindo pena dele.

Enquanto ela fazia a ligação telefônica, Rick estava confiante de que ele e Larry haviam conseguido fazer uma aliança estratégica de marketing. A empresa de Rick estava produzindo produtos para a manufatura e linha de montagem, itens que complementariam perfeitamente seu novo produto, o C2Alpha. Os produtos de Rick e o C2Alpha juntos formariam uma solução forte que abriria importantes mercados industriais para ambas as empresas.

Quando Jessica terminou de fazer a reserva para o último vôo da tarde, Rick pediu: "Bem. pelo menos posso falar com Steve se ele estiver disponível?" Mas Steve, vice-presidente e co-fundador da empresa, também não estava no escritório.

Rick, sendo muito amistoso com Jessica e flertando um pouco, sugeriu que, já que ele estava lá e que o seu vôo de volta seria no final da tarde, ele poderia levar algumas pessoas importantes para almoçar. E acrescentou: "Incluindo você é claro — há alguém que fica no seu lugar na hora do almoço?"

Ela ficou corada com a idéia de ser incluída e respondeu: "Quem você quer convidar?" Ele abriu novamente o seu palmtop e falou o nome de algumas pessoas — dois engenheiros de P&D, o homem novo de vendas e marketing e o funcionário de finanças designado para o projeto. Rick sugeriu que ela lhes dissesse sobre o seu relacionamento com a empresa e que ele gostaria de se apresentar a eles. Ele deu o nome do melhor restaurante da área, um lugar no qual Jessica sempre quis ir, e disse que reservaria a mesa ele mesmo para às 12h30 e ligaria mais tarde para ter certeza de que estava tudo certo.

Quando chegaram ao restaurante — os quatro mais Jessica — a sua mesa ainda não estava pronta e eles ficaram no bar. Rick deixou claro que a conta seria paga por ele. Rick era um homem com estilo e classe, o tipo de pessoa que faz você se sentir desde o início como se o conhecesse há anos. Sempre parecia saber a coisa certa a ser dita. tinha uma observação inteligente ou algo engraçado para dizer sempre que a conversa parecia acabar e fazia você se sentir bem pelo simples fato de estar ao seu lado.

Ele deu tantos detalhes sobre os produtos da sua própria empresa que eles podiam visualizar a solução conjunta de marketing sobre a qual ele parecia estar tão animado. Ele deu o nome de várias empresas da *Fortune 500* para as quais a sua empresa já estava vendendo, até que alguém da mesa começou a imaginar o seu produto se tornando um sucesso no dia em que as primeiras unidades saíssem da fábrica.

Em seguida, Rick começou a conversar com Brian, que era um dos engenheiros. Enquanto os outros conversavam entre eles, Rick trocou algumas idéias em particular com Brian e lhe falou dos recursos exclusivos do C2Alpha e daquilo que o distinguia de tudo o que a concorrência tinha. Ele ficou sabendo sobre alguns dos recursos que a empresa estava planejando e dos quais Brian tinha orgulho, dizendo que eles eram realmente "legais".

Rick foi conversando em particular com cada um deles. O rapaz de marketing teve a chance de falar sobre a data de lançamento e dos planos de marketing. E puxou um envelope do bolso e escreveu os detalhes dos custos de material e manufatura, o ponto de preço e a margem esperada, além do tipo de acordo que estava tentando fazer com cada um dos fornecedores, cujos nomes ele relacionou.

Quando terminou a conversa, Rick havia trocado idéias com todos que estavam na mesa e havia ganhado admiradores. No final da refeição, cada um deles cumprimentou Rick e agradeceu. Rick trocou cartões com cada um deles e, ao passar por Brian, o engenheiro, disse que queria ter uma discussão mais longa assim que Larry voltasse.

No dia seguinte. Brian atendeu Rick ao telefone. Este lhe disse que havia acabado de falar com Larry. "Vou voltar na segunda-feira para discutir alguns detalhes com ele", acrescentou Rick, "ele quer que eu me acostume logo com o seu produto. Disse para você enviar para ele os principais detalhes e especificações. Ele vai escolher algumas partes e vai mandar para mim por e-mail."

O engenheiro disse que estava tudo bem. "Bom", respondeu Rick. Ele continuou: "Larry falou que está tendo problemas para abrir suas mensagens de correio eletrônico. Em vez de enviar as informações para a sua conta regular, ele criou uma conta de correio eletrônico do Yahoo no centro de negócios do hotel. Ele disse para você enviar os arquivos para larryrobotics@yahoo.com."

Na manhã da segunda-feira seguinte, quando Larry entrou no escritório bronzeado e descansado, Jessica foi a primeira a falar de Rick. "Que rapaz ótimo! Ele levou vários de nós para almoçar inclusive eu". Larry pareceu confuso. "Rick? Quem é Rick?"

"Do que você está falando? O seu novo parceiro de negócios!"

"O quê!!!???"

"E todos ficaram tão impressionados com as perguntas que ele fez..."

"Eu não conheço nenhum Rick..."

"O que há com você? Isso é uma piada, Larry? Você está brincando comigo, não é?"

"Reúna a equipe executiva na sala de reuniões. *Agora.* Não importa o que eles estão fazendo. E também todos os que foram a esse almoço, incluindo você."

Eles sentaram-se ao redor da mesa com ar sombrio. Larry entrou, sentou-se e explicou: "Eu não conheço ninguém chamado Rick. Não tenho um novo parceiro de negócios que venho mantendo em segredo. Só há uma coisa óbvia que posso achar. Se há alguém fazendo piada entre nós, quero que essa pessoa fale *agora"*

Nenhum som. A sala parecia escurecer a cada segundo.

Finalmente Brian falou. "Por que você não disse alguma coisa quando lhe enviei aquele e-mail com as especificações do produto e o código-fonte?"

"Qual e-mail!?"

Brian empertigou-se. "Ah... droga!"

Cliff, o outro engenheiro, juntou a ele. "Ele nos deu seu cartão. Só temos de ligar para ele e ver o que está acontecendo."

Brian abriu seu palmtop, chamou uma entrada e passou o dispositivo para Larry. Ainda esperando um milagre, todos observaram enquanto Larry discava. Após um instante, ele apertou o botão do viva voz e todos ouviram um sinal de ocupado. Após tentar discar para o número várias vezes em 20 minutos, Larry, frustrado, discou para a telefonista e pediu uma interrupção de emergência.

Alguns momentos mais tarde, a telefonista voltou à linha. Ela disse: "Onde o senhor conseguiu esse número?" Larry disse que estava no cartão de um homem que ele precisava contatar com urgência. A telefonista disse: "Sinto muito. Esse é um número de teste da empresa de telefonia. Ele está sempre ocupado."

Larry começou a fazer uma lista das informações que haviam sido compartilhadas com Rick. O quadro não era nada bom.

Dois detetives da polícia vieram e fizeram um relatório. Após ouvir a história, disseram que nenhum crime estadual havia sido cometido; não havia nada que pudessem fazer. Eles aconselharam Larry a entrar em contato com o FBI porque eles têm jurisdição sobre todos os crimes que envolvem o comércio entre estados. Quando Rick Daggot pediu para o engenheiro encaminhar os resultados dos testes fazendo-se passar por outra pessoa, ele pode ter cometido um crime federal, mas Larry teria de falar com o FBI para descobrir isso.

Três meses mais tarde, Larry estava em sua cozinha lendo o jornal no café da manhã e quase derramou tudo. Aquilo que ele temia desde que ouviu falar pela primeira vez em Rick havia se tornado realidade, o seu pior pesadelo. Lá estava em letras grandes na primeira página da seção de negócios: uma empresa da qual ele nunca ouvira falar antes eslava anunciando o lançamento de um produto novo que parecia ser exatamente igual ao C2Alpha que a sua empresa vinha desenvolvendo nos dois últimos anos.

Por meio da fraude, essas pessoas o haviam derrotado no mercado. O seu sonho estava destruído. Os milhões de dólares investidos em pesquisa e desenvolvimento foram jogados fora. E ele provavelmente não poderia provar nada contra eles.

A história de Sammy Sanford

Bastante esperto para estar ganhando um bom salário em um emprego legítimo, mas trapaceiro o suficiente para preferir viver de golpes, Sammy Sanford havia se saído muito bem. Certa vez ele chamou a atenção de um espião que havia sido forçado a se aposentar cedo por causa de problemas com o álcool. Amargo e vingativo, o homem havia encontrado um modo de vender os talentos nos quais o governo o havia obrigado a se especializar. Sempre procurando pessoas que pudesse usar, ele havia identificado Sammy na primeira vez em que se encontraram. Sammy achou fácil e muito lucrativo mudar o foco de batedor de carteiras para batedor de segredos comerciais.

A maioria das pessoas não teria nervos para fazer o que faço. Tente enganar pessoas pelo telefone ou pela Internet e ninguém jamais o verá. Mas um bom golpista, aquele dos velhos tempos do tipo olho no olho (e ainda há muitos deles por aí, mais do que você pode imaginar), pode olhar você nos olhos, contar uma história c fazer com que você acredite nela. Conheço um ou dois promotores que acham que isso é crime. Acho que isso *é* um talento.

Mas você não pode fazer isso às cegas. Primeiro tem de fazer uma avaliação. Em um golpe de rua, você pode tirar a temperatura de um homem com um pouco de conversa e algumas sugestões bem articuladas. Consiga as respostas corretas e pronto! — você enganou um bobo.

Um emprego em uma empresa *é* aquilo que chamamos de um grande golpe. Você tem de se preparar bem. Descubra quais são os botões certos e o que querem. Do que precisam. Planeje um ataque. Seja paciente e faça a sua lição de casa. Descubra o papel que você vai desempenhar e decore o seu texto. E não vá lá antes de estar preparado.

Passei mais de três semanas me preparando para este golpe. Tive uma sessão de dois dias sobre aquilo que eu diria que a "minha" empresa faz e sobre como descrever o motivo pelo qual essa seria uma boa aliança de marketing.

Em seguida, tive sorte. Liguei para a empresa e disse que era de uma empresa de capital de risco e que estávamos interessados em marcar uma reunião e estava tentando descobrir um dia em que todos os nossos sócios estivessem disponíveis nos próximos meses e se havia alguma época que deveria evitar, algum período em que Larry não estaria na cidade. E ela respondeu: "Sim. ele ainda não tirou férias em dois anos desde que abriu a empresa, mas a sua mulher o estava arrastando de férias para jogar golf na primeira semana de agosto."

Faltavam apenas duas semanas e eu podia esperar.

Nesse meio tempo uma revista especializada me deu o nome da empresa de RP da companhia. Disse que gostei do espaço que eles estavam conseguindo para o seu cliente fabricante de robótica e queria falar com a pessoa que atendia aquela conta para que ela cuidasse da minha empresa. Essa pessoa era uma jovem cheia de energia que gostava da idéia de conseguir uma conta nova. Com um almoço caro e um drink a mais do que ela realmente queria, ela fez o que pôde para me convencer de que eles eram muito bons para entender os problemas de um cliente e encontrar as soluções certas de RR Joguei alto para convencê-la. Precisava ter alguns detalhes. Com algumas cutucadas quando os pratos estavam sendo retirados, ela já havia me contado mais sobre o novo produto e os problemas da empresa do que jamais havia esperado.

A coisa estava dando certo como um relógio. A história de estar muito embaraçado com o fato de que a reunião era na próxima semana, mas que eu também poderia aproveitar para almoçar com a equipe foi engolida pela recepcionista. Ela até sentiu pena de mim. O almoço me custou ao todo US$ 150,00, incluindo o serviço. E consegui o que precisava. Os números de telefones, os cargos e uma das pessoas-chave que acreditava que eu era quem dizia ser.

Brian havia me enganado. Ele parecia o tipo de pessoa que apenas me mandaria por e-mail algo que eu pedisse. Mas parecia que ele estava escondendo alguma coisa quando falei no assunto. Vale a pena esperar pelo inesperado. Aquela conta de e-mail no nome de Larry eu tinha no bolso do colete só para o caso de precisar. O pessoal de segurança do Yahoo provavelmente ainda está esperando que alguém use a conta novamente para que eles possam rastreá-lo. Eles terão de esperar muito. A prima dona já cantou. E já estou em outro projeto.

Analisando a trapaça

Todos os que realizam um golpe pessoalmente têm de usar uma aparência que o faça ser aceito. Ele vai se produzir de uma forma para aparecer em uma pista de corridas, de outra forma para aparecer em um parque aquático local e de outra forma ainda para aparecer em um bar de algum hotel cinco estrelas.

Na espionagem industrial as coisas funcionam da mesma maneira. Um ataque pode pedir terno. gravata e uma pasta cara se o espião está se fazendo passar por um executivo de uma empresa estabelecida, um consultor ou um representante de vendas. Em outra função, ao tentar se fazer passar por um engenheiro de software, um técnico ou alguém do departamento de correspondência, as roupas, o uniforme — enfim, toda a aparência — seria diferente.

Para se infiltrar na empresa, o homem que se chamou de Rick Daggot sabia que tinha de projetar uma imagem de confiança e competência, a qual seria suportada por um conhecimento completo do produto da empresa e da indústria.

Ele não teve muita dificuldade para se apossar das informações que precisava ter com antecedência. E também criou um golpe fácil de aplicar quando o CEO estivesse fora. Um pequeno desafio. mas mesmo assim não muito difícil, seria encontrar detalhes suficientes sobre o projeto para que ele

parecesse estar "por dentro" daquilo que eles estavam fazendo. Quase sempre essas informações são conhecidas dos diversos fornecedores da empresa, bem como dos investidores, capitalistas de risco que eles contataram para levantar o dinheiro, seu banqueiro e a sua empresa de advocacia. O atacante tem de tomar cuidado, porém. Pode ser difícil encontrar alguém que entrará com o conhecimento interno, mas tentar duas ou três fontes para encontrar alguém que possa dar as informações pode fazer com que as pessoas descubram o golpe. E aí que está o perigo. Os Rick Daggost da vida precisam escolher com cuidado e trilhar o caminho de cada informação apenas uma vez.

O almoço foi outra proposição arriscada. Primeiro havia o problema de organizar tudo para que ele tivesse alguns minutos sozinho com cada pessoa, fora do alcance dos ouvidos dos outros. Ele disse a Jessica que o horário seria 12h30, mas fez a reserva da mesa para 13h00 em um restaurante caro. Ele esperava que eles ficariam no bar tomando uns drinques e foi isso exatamente o que aconteceu. Uma oportunidade perfeita para conversar com cada indivíduo.

Mesmo assim, havia muitas chances de algo dar errado. Uma resposta errada ou uma observação descuidada poderiam revelar que Rick era um impostor. Apenas um espião industrial extremamente confiante e ardiloso se arriscaria a expor-se dessa maneira. Mas anos de trabalho nas ruas como esse haviam aumentado as habilidades e a confiança de Rick para que, mesmo que cometesse um deslize, ele pudesse se recuperar bem o suficiente para não levantar suspeitas. Essa era a parte mais difícil, o momento mais perigoso de toda a operação e a adrenalina que sentiu ao realizar um golpe como esse fez com que percebesse que não precisava dirigir carros de corrida, fazer surf aéreo ou enganar a sua mulher — ele já tinha emoção suficiente no seu trabalho. Ele se perguntava quantas pessoas poderiam dizer o mesmo?

Recado do Mitnick

Embora a maioria dos ataques da engenharia social ocorra pelo telefone ou e-mail, você não deve supor que um atacante audacioso nunca aparecerá em pessoa na sua empresa. Na maioria dos casos, o impostor usa alguma forma de engenharia social para ter acesso a um prédio após falsificar o crachá de um empregado usando um programa de software comum como o Photoshop.

E os cartões com o número da linha de teste da empresa de telefonia? A série de televisão *Arquivo Confidencial,* sobre um detetive particular, ilustrava uma técnica inteligente e meio engraçada. Rockford (interpretado pelo ator James Garner) tinha uma impressora portátil para cartões em seu carro, a qual ele usava para imprimir um cartão apropriado para aquilo que a ocasião pedia. Hoje em dia, um engenheiro social pode imprimir cartões em uma hora em qualquer copiadora, ou pode imprimi-los em uma impressora a laser.

O que leva um grupo de homens e mulheres inteligentes a aceitarem um impostor? Dimensionamos uma situação com o instinto e com o intelecto. Se a história convence, essa é a parte do intelecto, e se um golpista consegue projetar uma imagem de credibilidade, estamos dispostos a baixar a guarda. A imagem de credibilidade separa um golpista de sucesso ou engenheiro social de alguém que rapidamente está atrás das grades.

Pergunte a si mesmo: o que me dá certeza de que nunca cairia em uma história como a de Rick? Se você tem certeza que não, pergunte a si mesmo se alguém já tentou enganá-lo. Se a resposta da segunda pergunta for sim. provavelmente essa também é a resposta correta para a primeira pergunta.

Observação

John Le Carré, autor do livro O *Espião que Veio do Frio, Um Espião Perfeito* e de muitos outros livros notáveis, cresceu como o filho de um educado golpista que viveu muito tempo. Quando criança, Le Carré ficou chocado ao descobrir que, embora bem-sucedido para enganar as outras pessoas, seu pai também era crédulo e mais de uma vez foi vítima de outro golpista. Isso só prova que todos correm o risco de serem enganados por um engenheiro social, mesmo outro engenheiro social.

JOGO DE ENGANAÇÃO

Agora temos um desafio. A próxima história não envolve a espionagem industrial. Ao ler esta parte, veja se pode entender o motivo pelo qual resolvi incluir este capítulo!

Harry Tardy voltou para casa e estava amargurado. Os Fuzileiros Navais pareciam uma ótima fuga até que foi expulso do campo de combate. Agora ele voltara para a cidade natal que odiava, estava fazendo cursos de computador na escola comunitária local e procurando um modo de atacar o mundo.

Finalmente ele chegou a um plano. Depois de beber algumas cervejas com um colega de classe, ele reclamava do instrutor, que era do tipo sabe tudo e sarcástico. Juntos resolveram criar um esquema perverso para queimar o professor: eles pegariam o código-fonte de um conhecido personal digital assistam (PDA) e o enviariam para o computador do instrutor e deixariam pistas para que a empresa pensasse que o instrutor era o culpado.

O novo amigo, Karl Alexander, disse que "conhecia alguns truques" e diria a Harry como fazer as coisas. E eles continuaram com o plano.

Fazendo a lição de casa

Um pouco de pesquisa inicial mostrou a Harry que o produto linha sido criado no Centro de Desenvolvimento localizado na sede do fabricante do PDA fora do país. Mas também havia uma instalação de P&D nos Estados Unidos. Karl disse que isso era bom. Para que uma tentativa funcione, tem de haver alguma instalação da empresa nos EUA, a qual também precise acessar o código-fonte.

Nesse ponto Harry estava pronto para ligar para o Centro de Desenvolvimento no exterior. Foi aqui que um pedido de simpatia entrou em cena: "Ah, querida, estou com problemas e preciso de ajuda, por favor, me ajude." Naturalmente o pedido foi um pouco mais sutil do que isso. Karl escreveu um script, mas Harry parecia completamente falso tentando usá-lo. No final, ele praticou com Karl para que pudesse dizer aquilo que precisava em tom coloquial.

Finalmente Harry disse (com Karl sentado ao seu lado) algo mais ou menos assim:

"Estou ligando do P&D de Minneapolis. O nosso servidor teve um worm que infectou lodo o departamento. Tivemos de instalar o sistema operacional novamente e, em seguida, tivemos de restaurar o backup, mas nenhum deles serviu. Adivinha quem deveria ter verificado a integridade dos backups? Eu, é claro. Assim sendo, meu chefe está gritando comigo e a gerência está querendo se matar porque perdemos os dados. Olhe, preciso ter a revisão mais recente do diretório do código-fonte o mais rápido possível. Preciso que você compacte os arquivos em formato *gzip* e o envie para mim".

Jargão

GZIP Classificar arquivos em um único arquivo compactado usando o utilitário GNU do Linux.

Nesse ponto Karl escreveu uma nota para Harry e este disse ao homem que estava no outro lado da linha que ele só queria que ele transferisse o arquivo internamente para o departamento de P&D de Minneapolis. Isso era muito importante: quando o homem do outro lado da linha verificou que ele só precisava enviar o arquivo para outra parte da empresa, a sua mente sossegou — o que poderia haver de errado nisso?

Ele concordou em fazer um gzip e enviá-lo. Passo a passo, com Karl do lado, Harry ensinou o interlocutor a iniciar o procedimento de compactação do enorme código-fonte em um único arquivo compacto. Ele também deu um nome de arquivo a ser usado no arquivo compactado ("newdata") e explicou que esse nome evitaria qualquer confusão com os arquivos antigos e corrompidos.

Karl teve de explicar a próxima etapa duas vezes antes que Harry a entendesse, mas isso foi crucial para o joguinho de enganação que Karl havia criado. Harry devia ligar para o R&D em Minneapolis e dizer para alguém: "Quero enviar um arquivo para você e, em seguida, quero que você o envie para outro lugar para mim" — obviamente tudo isso estaria cheio de motivos que tornariam a coisa toda plausível. O que confundia Harry era que ele deveria dizer: *"Vou* enviar um arquivo para você" quando ele não ia enviar nada. Ele tinha de fazer o rapaz com quem ele estava falando no Centro de P&D achar que o arquivo vinha dele. quando aquele Centro realmente iria receber o arquivo com o código-fonte proprietário da Europa. "Por que eu diria para ele que está vindo de mim quando realmente está vindo de fora do país?" Harry queria saber.

"O funcionário do Centro de P&D é só um parafuso", explicou Karl. "Ele tem de achar que está apenas fazendo um favor para um colega aqui dos EUA recebendo um arquivo de você e, em seguida, encaminhando esse arquivo para você."

Harry finalmente entendeu. Ele ligou para o Centro de P&D, pediu que a recepcionista ligasse para o Centro de Computadores e quis falar com um operador de computador. O rapaz que atendeu parecia tão jovem quanto o próprio Harry. Harry o cumprimentou, explicou que estava ligando da divisão de desenvolvimento de Chicago da empresa e que tinha um arquivo que estava tentando enviar para um dos seus colegas que estava trabalhando com ele em um projeto, mas "Tivemos um problema de roteador e não podemos acessar a rede. Gostaria de transferir o arquivo para você e depois que você recebê-lo, ligo de volta para dizer como transferir esse arquivo para o computador do meu colega."

Até aqui tudo bem. Em seguida, Harry perguntou ao jovem se o seu centro de computadores tinha uma conta *de FTP anônimo,* uma configuração que permite que todos transfiram e recebam arquivos de um diretório no qual uma senha é requerida. Sim, havia um FTP anônimo disponível e ele deu a Harry o endereço interno Internet Protocol (IP) para acessá-lo.

Com essas informações, Harry ligou de volta para o Centro de Desenvolvimento no exterior. O arquivo compactado já estava pronto e Harry deu as instruções para a transferência do arquivo para o site de FTP anônimo. Em menos de cinco minutos, o arquivo com o código-fonte compactado foi enviado para o garoto do Centro de P&D.

Jargão

FTP ANÔNIMO Um programa que fornece acesso a um computador remoto mesmo que você não tenha uma conta e que use o File Transfer protocol (FTP). Embora o FTP anônimo possa ser acessado sem uma senha, em geral os direitos de acesso de usuário a determinadas pastas são restritos.

Definindo a vítima

Eles estavam a meio caminho de realizar o seu objetivo. Agora Harry e Karl tinham de esperar para ter certeza de que o arquivo havia chegado antes de continuar. Durante a espera, eles foram até a mesa do instrutor no outro lado da sala e cuidaram de duas outras etapas necessárias. Primeiro eles configuraram um servidor de FTP anônimo, o qual serviria como destino para o arquivo na última parte do seu esquema.

A segunda etapa forneceu uma solução para um problema que de outra maneira seria difícil de resolver. É claro que eles não podiam dizer para o homem do Centro de P&D para que enviasse o arquivo para um endereço do tipo warren@rms.ca.edu. O domínio ".edu" seria uma rua sem saída, uma vez que todo operador meio atento de computadores reconheceria esse endereço com sendo o endereço de uma escola e toda a operação estaria condenada. Para evitar isso eles entraram no Windows do computador do instrutor e viram o endereço IP da máquina, o qual eles dariam como o endereço para o envio do arquivo.

Nesse ponto estava na hora de ligar de volta para o operador de computador do Centro de P&D. Harry ligou: "Acabei de transferir o arquivo do qual lhe falei. Você pode ver se recebeu?" Sim, ele havia chegado. Harry pediu para ele tentar encaminhar o arquivo e deu o endereço IP. Ele ficou ao telefone enquanto o jovem fazia a conexão e começava a transmitir o arquivo e eles observaram a luz da unidade de disco piscando no computador do instrutor — recebendo animadamente o download.

Harry trocou algumas observações com o rapaz sobre como um dia os computadores e periféricos seriam mais confiáveis, agradeceu *e* disse adeus.

Os dois copiaram o arquivo da máquina do instrutor para dois discos Zip, um para cada um deles. Isso era como roubar um quadro que você gosta de um museu, mas não se atrever a mostrar para os seus amigos. Exceto que neste caso era mais provável que eles tivessem feito uma duplicata da pintura original e o museu ainda tinha o seu próprio original.

Em seguida, Karl ensinou a Harry como remover o servidor de FTP da máquina do instrutor e apagar o controle de auditoria para que não houvesse evidencia daquilo que fizeram — apenas o arquivo roubado que foi deixado lá para ser facilmente localizado.

Em uma última etapa eles publicaram uma seção do código-fonte na Usenet diretamente do computador do instrutor. Apenas uma seção, para que não causassem grandes danos à empresa, mas deixando pistas claras que levavam diretamente ao instrutor. Ele teria dificuldades em explicar tudo aquilo.

Analisando a trapaça

Embora vários elementos tenham sido combinados para que esse golpe funcionasse, ele não teria tido sucesso sem alguma simpatia e habilidade em pedir ajuda: "Meu chefe está gritando comigo e o

gerenciamento está querendo se matar". Isso. combinado a uma explicação exata de como o homem do outro lado da linha poderia ajudar a resolver o problema, resultou em um golpe poderoso e convincente. Essa combinação funcionou aqui e muitas outras vezes.

O segundo elemento crucial foi que o homem que entendia o valor do arquivo tinha de enviá-lo para um endereço *dentro* da empresa.

E a terceira peça do quebra-cabeça: o operador do computador podia ver que o arquivo havia sido transferido para ele de dentro da empresa. Isso só podia significar — ou pelo menos assim parecia — que o homem que o enviou podia tê-lo enviado para o destino final, não fosse a conexão de rede externa que não estava funcionando. Que mal faria ao ajudar o homem, enviando o arquivo para ele?

Mas e quanto a dar um nome diferente para o arquivo compactado? Isso parecia um detalhe, mas ele era importante. O atacante não podia se dar ao luxo de arriscar receber o arquivo com um nome que o identificasse como o código-fonte, ou com nome relacionado com o produto. Uma solicitação para enviar um arquivo com um nome como aquele para fora da empresa podia ter feito soar os alarmes. Era crucial fazer com que o arquivo fosse rotulado com um nome inofensivo. Como os atacantes previram, o segundo jovem não viu problemas em enviar o arquivo para fora da empresa. Um arquivo com um nome como "dados novos", sem dar nenhuma pista sobre a verdadeira natureza das informações, dificilmente levantaria suspeitas.

Por fim, você descobriu o que esta história está fazendo em um capítulo dedicado à espionagem industrial? Se não descobriu, aqui está a resposta. Aquilo que os dois alunos fizeram para pregar uma peça poderia ter sido feito facilmente por um espião industrial profissional, talvez pago por um concorrente ou por um governo estrangeiro. De qualquer forma, o dano poderia ter sido devastador para a empresa, diminuindo seriamente as vendas do seu novo produto quando o produto do concorrente chegasse ao mercado.

Recado do Mitnick

A regra básica que todo empregado deve ter clara em sua cabeça é que, exceto com a aprovação do gerenciamento, você não deve transferir arquivos para pessoas que não conhece pessoalmente, mesmo que o destino pareça estar dentro da rede interna da sua empresa.

Com que facilidade o mesmo tipo de ataque poderia ter sido executado na sua empresa?

EVITANDO A TRAPAÇA

Agora que a Guerra Fria terminou, a espionagem industrial, que há muito tem sido um desafio para as empresas, agora se tornou o prato principal dos espiões que concentram seus esforços na obtenção de segredos comerciais cobrando um bom preço. Os governos estrangeiros e as corporações estão usando espiões industriais freelance para roubar as informações. As empresas domésticas também contratam corretores de informações que cruzam a linha entre o legal e o ilegal em seus esforços para obter a inteligência da concorrência. Em muitos casos esses espiões são ex-militares que se transformaram em corretores de informações industriais e que têm o pré-requisito do conhecimento e da experiência para explorar facilmente as organizações, em particular aquelas que não tomam precauções para proteger suas informações e educar o seu pessoal.

A segurança externa

O que poderia ter ajudado a empresa com problemas nas suas instalações externas de armazenamenlo? O perigo aqui teria sido evitado se a empresa tivesse criptografado seus dados. Sim, a criptografia exige tempo e despesas extras, mas o esforço é recompensado. Os arquivos criptografados precisam ser verificados regularmente para que se tenha a certeza de que a criptografia/decriptografia está funcionando bem.

Sempre há o perigo de que as chaves de criptografia se percam ou de que a única pessoa que conhece as chaves seja atingida por um ônibus. Mas o nível de aborrecimento pode ser minimizado, e todos aqueles que armazenam as informações confidenciais externamente em uma empresa comercial e não usam a criptografia são, me desculpem o termo, uns idiotas. Isso é como caminhar em uma vizinhança perigosa com uma nota de US$ 20,00 saindo do bolso e pedindo para ser roubada.

Deixar mídia de backup em um lugar onde alguém pode entrar e tirá-la é uma falha de segurança comum. Há vários anos, trabalhava em uma empresa que poderia ter se esforçado mais para proteger as informações dos clientes. A equipe da operação deixava as fitas de backup da empresa *fora* da porta da sala trancada dos computadores para que um mensageiro as pegasse no outro dia. Todos poderiam sair com as fitas de backup, as quais continham todos os documentos de processador de texto da empresa em texto não criptografado. Se os dados de backup estão criptografados, a perda do material é um aborrecimento; se eles não estão criptografados — bem. você pode imaginar o impacto sobre a sua empresa melhor do que eu.

A necessidade que as empresas maiores têm de armazenamento externo confiável é vital. Mas os procedimentos de segurança da sua empresa precisam incluir uma investigação na empresa de armazenamento para saber se eles estão conscientes das suas próprias políticas e procedimentos de segurança. Se eles não forem tão dedicados quanto a sua própria empresa, todos os seus esforços de segurança podem ir por água abaixo.

As empresas menores têm uma boa alternativa para o backup. Elas podem enviar os arquivos novos e alterados a cada noite para uma das empresas que oferecem o armazenamento on-line. Aqui também é essencial que os dados sejam criptografados. Caso contrário, as informações estarão disponíveis não apenas para um empregado desleixado da empresa de armazenamento, mas também para todo invasor de computador que invada os sistemas de computadores ou a rede da empresa de armazenamento on-line.

Obviamente, ao configurar um sistema de criptografia para proteger a segurança dos seus arquivos de backup, que você também deve configurar um procedimento altamente seguro para armazenar as chaves de criptografia e as frases de password que as desbloqueiam. As chaves secretas usadas para criptografar os dados devem ser armazenadas em um cofre ou caixa forte. A prática-padrão da empresa precisa prever a possibilidade de o empregado que lida com esses dados sair repentinamente, morrer ou assumir outro cargo. Sempre deve haver pelo menos duas pessoas que conhecem o local de armazenamento e os procedimentos de criptografia/decriptografia, bem como a políticas que determinam como e quando as chaves devem ser alteradas. As políticas também devem exigir que as chaves de criptografia sejam alteradas imediatamente quando um empregado que tinha acesso a elas for embora.

Quem é ele?

O exemplo de um artista da trapaça deste capítulo que usa seu charme para fazer com que os empregados revelem informações reforça a importância da verificação da identidade. A solicitação de

encaminhamento do código-fonte para um site FTP também destaca a importância de conhecer a pessoa que faz a solicitação.

No Capítulo 16 você encontra as políticas especificas para a verificação da identidade de um estranho que faz uma solicitação de informações ou pede que alguma ação seja executada. Já falamos da necessidade da verificação em todo este livro. No Capítulo 16 você terá os detalhes de como isso deve ser feito.

parte 4

Eliminando as Barreiras

Capítulo 15

Conscientização e Treinamento em Segurança da Informação

Um engenheiro social recebeu a atribuição de obter os planos do seu novo produto que deve ser lançado em dois meses. O que vai impedi-lo?

O seu firewall? Não.

Dispositivos avançados de autenticação? Não.

Sistemas detectores de invasão? Não.

Criptografia? Não.

Acesso limitado aos números de telefone de discagem por modems? Não.

Nomes de código nos servidores para dificultar que um estranho determine qual servidor pode conter os planos do produto? Não.

A verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social.

A SEGURANÇA POR MEIO DA TECNOLOGIA, DO TREINAMENTO E DOS PROCEDIMENTOS

As empresas que realizam testes de penetração de segurança relatam que suas tentativas de invadir os sistemas de computadores de uma empresa cliente com métodos da engenharia social têm um índice de sucesso de quase *100 por cento.* As tecnologias de segurança podem dificultar esses tipos de ataques retirando as pessoas do processo de tomada de decisão. Entretanto, o único meio verdadeiramente efetivo de amenizar a ameaça da engenharia social e usar a conscientização para a segurança *combinada a* políticas de segurança que definem as principais regras para o comportamento do empregado, junto com sua educação e treinamento.

Só existe uma maneira de manter seguros os seus planos de produto: ter uma força de trabalho treinada e consciente. Isso envolve o treinamento nas políticas e procedimentos, mas também — e provavelmente mais importante — um programa constante de conscientização. Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização.

A primeira etapa é fazer com que todos os que trabalham na empresa tenham consciência de que existem pessoas inescrupulosas que usarão a fraude para manipulá-las psicologicamente. Os empregados devem ser educados sobre as informações que precisam ser protegidas e sobre como protege-

las. Depois que as pessoas entendem melhor como podem ser manipuladas, elas estão em melhor posição de reconhecer um ataque que está para ser realizado.

A consciência da segurança também significa educar a todos sobre as políticas e os procedimentos de segurança da empresa. Como discutiremos no Capítulo 16, as políticas são regras necessárias para orientar o comportamento do empregado para que ele proteja os sistemas corporativos de informações e as informações confidenciais.

Este capítulo e o próximo fornecem um mapa de segurança que pode salvá-lo de ataques caros. Se você não tiver empregados treinados e alertas seguindo bons procedimentos, a questão não é *se*, mas sim *quando* você perderá informações valiosas para um engenheiro social. Não espere que um ataque aconteça para depois instituir essas políticas. Isso seria devastador para o bem-estar da sua empresa e dos seus empregados.

ENTENDENDO COMO OS ATACANTES APROVEITAM-SE DA NATUREZA HUMANA

Para desenvolver um programa de treinamento bem-sucedido, antes de tudo você deve entender o motivo pelo qual as pessoas são vulneráveis aos ataques. Ao identificar essas tendências no seu treinamento — por exemplo, chamando a atenção para eles nas discussões dramatizadas — você pode ajudar seus empregados a entender o motivo pelo qual todos nós podemos ser manipulados pelos engenheiros sociais.

A manipulação tem sido estudada pelos cientistas há pelo menos 50 anos. Robert B. Cialdini, ao escrever para a revista *Scientific American* (edição de fevereiro de 2001), resumiu a sua pesquisa apresentando "seis tendências básicas da natureza humana", as quais estão envolvidas em uma tentativa de obter o consentimento para uma solicitação.

Essas seis tendências são usadas pelos engenheiros sociais (algumas conscientemente e, com mais freqüência, outras inconscientemente) em suas tentativas de manipulação.

Autoridade

As pessoas têm a tendência de atender a uma solicitação que é feita por uma pessoa com autoridade. Como já discutimos em outra parte deste livro, uma pessoa pode ser convencida a atender a uma solicitação se ela acreditar que o solicitante é uma pessoa com autoridade ou que está autorizada a fazer tal solicitação.

Em seu livro *Influence*, o Dr. Cialdini escreve um estudo sobre três hospitais do meio-oeste nos quais 22 estações separadas de enfermagem foram contatadas por um interlocutor que dizia ser um médico do hospital e receberam instruções para administrar uma droga controlada para um paciente daquela ala. As enfermeiras que receberam essas instruções não conheciam o interlocutor. Elas nem mesmo sabiam se ele era realmente um médico (e ele não era). Elas receberam as instruções pelo telefone, o que violava a política do hospital. O "médico" disse para elas administrarem uma droga cujo uso não era autorizado naquela ala, e a dosagem que ele disse para elas administrarem era o dobro da dosagem diária máxima e, assim, poderia ter colocado a vida do paciente em risco. Mesmo assim, em 95% dos casos, como relatou Cialdini, "a enfermeira obteve a dosagem necessária na sala de remédios da ala e estava indo administrá-la ao paciente" antes de ser interceptada por um observador que lhe contou sobre a experiência.

Exemplos de ataques: um engenheiro social tenta impor autoridade alegando ser do departamento de TI ou dizendo ser um executivo ou uma pessoa que trabalha para um executivo da empresa.

Afabilidade

As pessoas têm a tendência de atender uma pessoa que faz uma solicitação quando ela conseguiu se fazer passar por alguém agradável ou com interesses, crenças e atitudes semelhantes aos da vítima.

Exemplos de ataques: por meio da conversação, o atacante consegue descobrir um hobby ou interesse da vítima e diz ser interessado ou entusiasmado pelo mesmo hobby ou interesse. Ou então alega ser do mesmo estado ou escola ou ter objetivos semelhantes. O engenheiro social também tentará imitar os comportamentos do seu alvo para criar a aparência de semelhança.

Reciprocidade

Podemos atender automaticamente a uma solicitação quando recebemos ou temos a promessa de receber algo de valor. O presente pode ser um item material, um conselho ou ajuda. Quando alguém fez algo para você, você sente uma inclinação a retribuir. Essa forte tendência de retribuir existe nas situações em que a pessoa que recebe o presente não pediu por ele. Uma das maneiras mais eficazes de influenciar as pessoas para nos fazer um "favor" (atender a uma solicitação) é dar algum presente ou auxílio que se constitui em uma obrigação implícita.

Os membros do culto religioso Hare Krishna conseguiam ser muito eficazes ao influenciar as pessoas a fazerem doações para a sua causa dando primeiro um livro ou uma flor de presente. Se o destinatário tentasse devolver o livro, eles recusavam e observavam: "Este é o nosso presente para você." Esse princípio comportamental de reciprocidade era usado pelos Krishnas para aumentar de forma substancial as doações.

Exemplo de ataque: um empregado recebe uma ligação de uma pessoa que se identifica como sendo do departamento de TI. O interlocutor explica que alguns computadores da empresa foram infectados por um vírus novo que não é reconhecido pelo software antivírus e que pode destruir todos os arquivos de um computador. Ele se oferece para instruir a pessoa a tomar algumas medidas para evitar problemas. Depois disso, o interlocutor pede que a pessoa teste um utilitário de software que acabou de ser atualizado recentemente, o qual permite que os usuários mudem as senhas. O empregado reluta em recusar, porque o interlocutor acabou de prestar ajuda que supostamente o protege contra um vírus. Ele retribui, atendendo à solicitação do interlocutor.

Consistência

As pessoas têm a tendência de atender após fazer um comprometimento público ou adotar uma causa. Depois que prometemos, faremos qualquer coisa, não queremos parecer pouco confiáveis ou indesejáveis e tendemos a seguir as instruções para sermos coerentes com nossa declaração ou promessa.

Exemplo de ataque: o atacante entra em contato com uma funcionária relativamente nova e a aconselha sobre o acordo para seguir determinadas políticas e procedimentos de segurança como uma condição para usar os sistemas de informações da empresa. Após discutir algumas

práticas de segurança, o interlocutor pede à usuária para fornecer a sua senha "para verificar se ela entendeu" a política sobre selecionar uma senha difícil de adivinhar. Depois que a usuária revela a sua senha, o interlocutor faz uma recomendação para que ela crie senhas para que **o** atacante possa adivinhá-las. A vítima atende por causa do seu acordo anterior de seguir as políticas de segurança e porque supõe que o interlocutor está apenas verificando o seu entendimento.

Validação social

As pessoas tendem a cooperar quando isso parece estar de acordo com aquilo que as outras pessoas estão fazendo. A ação dos outros é aceita como uma validação de que o comportamento em questão está correto e apropriado.

Exemplo de ataque: o interlocutor diz que está realizando uma pesquisa e dá o nome das outras pessoas do departamento que diz já terem cooperado com ele. A vítima, acreditando que a cooperação dos outros valida a autenticidade da solicitação, concorda em tomar parte. Em seguida, o interlocutor faz uma série de perguntas, entre as quais estão perguntas que levam a vítima a revelar o seu nome de usuário e senha.

Escassez

As pessoas têm a tendência de cooperar quando acreditam que o objeto procurado está em falta e que outras pessoas estão competindo por ele, ou que **ele** só está disponível por um período de tempo curto.

Exemplo de ataque: o atacante envia e-mails dizendo que as primeiras 500 pessoas que se registrarem no novo site Web da empresa ganharão ingressos grátis para *a premiere* de um filme a que todos querem assistir. Quando um empregado desavisado se registra no site, ele tem de fornecer o endereço de e-mail da sua empresa e selecionar uma senha. Muitas pessoas, motivadas pela conveniência, têm a tendência de usar a mesma senha ou uma senha semelhante em todo sistema de computador que usam. Aproveitando-se disso, o atacante tenta comprometer o trabalho do alvo **e** os sistemas de computadores domésticos com o nome de usuário **e a** senha que foram inseridos durante o processo de registro no site Web.

CRIANDO PROGRAMAS DE TREINAMENTO E DE CONSCIENTIZAÇÃO

O seu risco não diminui com o simples fato de você criar um panfleto sobre a política de segurança ou enviar seus empregados para uma página da intranet que detalha as políticas de segurança. As empresas devem não apenas definir por escrito as regras das políticas, mas também devem se esforçar ao máximo para orientar *todos* os que trabalham com as informações corporativas ou com os sistemas de computadores para que eles aprendam e sigam as regras. Além disso, você deve garantir que todos entendam o motivo de cada política, para que as pessoas não tentem se desviar da regra por questões de conveniência. Caso contrário, a ignorância sempre será a melhor desculpa do empregado, e é exatamente essa vulnerabilidade que os engenheiros sociais vão explorar.

O objetivo central de um programa de conscientização sobre segurança é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a *querer*

entrar no programa e fazer a sua parte para proteger os ativos de informações da organização. Um ótimo motivador nesse caso é explicar como a participação das pessoas beneficiará não apenas a empresa, mas também os empregados individuais. Como a empresa detém determinadas informações particulares sobre cada funcionário, quando os empregados fazem a sua parte para proteger as informações ou os sistemas de informações, na verdade eles estão protegendo também as suas próprias informações.

Um programa de treinamento em segurança requer um suporte substancial. O esforço de treinamento precisa atingir cada pessoa que tem acesso a informações confidenciais ou aos sistemas corporativos de computadores, deve ser contínuo e ser sempre revisado para atualizar o pessoal sobre as novas ameaças e vulnerabilidades. Os empregados devem ver que a direção está totalmente comprometida com o programa. Esse comprometimento deve ser real, e não apenas um memorando com um carimbo que diz "Nós dizemos amém". E o programa deve ser fundamentado por recursos suficientes para desenvolver, comunicar, testar e medir o sucesso.

Objetivos

A orientação básica que deve ser lembrada durante o desenvolvimento de um programa de treinamento e conscientização em segurança é que o programa precisa se concentrar em criar em todos os empregados a consciência de que a sua empresa pode ser atacada a qualquer momento. Eles devem aprender que cada empregado tem um papel na defesa contra qualquer tentativa de entrar nos sistemas de computadores ou de roubar dados confidenciais.

Como muitos aspectos da segurança das informações envolvem a tecnologia, é muito fácil para os empregados acharem que o problema está sendo tratado por firewalls e por outras tecnologias de segurança. Um dos objetivos principais do treinamento deve ser a criação em cada empregado da consciência de que eles são a linha de frente necessária para proteger a segurança geral da organização.

O treinamento em segurança deve ter um objetivo significativamente maior do que simplesmente impor regras. O criador do programa de treinamento deve reconhecer a forte tentação dos empregados sob pressão de fazer seus trabalhos e de ignorar suas responsabilidades de segurança. O conhecimento das táticas da engenharia social e de como se defender dos ataques é importante, mas não servirá para nada se o treinamento não se concentrar bastante na *motivação* dos empregados para que usem o conhecimento.

A empresa pode considerar que o programa está atingindo o seu objetivo final se todos os que realizarem o treinamento estiverem convencidos e motivados por uma noção básica: a noção de que a segurança das informações faz parte do seu trabalho.

Os empregados devem refletir e aceitar que a ameaça dos ataques da engenharia social é real e que uma perda de informações confidenciais da empresa pode ameaçar a empresa e também as suas informações pessoais e os seus empregos. De certa forma, não cuidar da segurança das informações no trabalho é o mesmo que não cuidar do cartão de banco ou do número do cartão de crédito de alguém. Essa pode ser uma analogia convincente para criar o entusiasmo pelas práticas de segurança.

Estabelecendo o programa de treinamento e conscientização

A pessoa responsável pela criação do programa de segurança das informações precisa reconhecer que esse não é um projeto de "tamanho único". Pelo contrário, o treinamento precisa ser desenvolvido para se adequar aos requisitos específicos de diversos grupos dentro da empresa. Embora muitas das

políticas de segurança destacadas no Capítulo 16 apliquem-se a todos os empregados da empresa, muitas outras são exclusivas. No mínimo, a maioria das empresas precisará de programas de treinamento adaptados a esses grupos distintos: os gerentes, o pessoal de TI, os usuários de computadores, o pessoal das áreas não técnicas, os assistentes administrativos, os recepcionistas e o pessoal de segurança. (Consulte a divisão das políticas por função no Capítulo 16.)

Como o pessoal da segurança de uma empresa normalmente não deve ser proficiente em computadores, e, exceto talvez de uma forma muito limitada não entre em contato com os computadores da empresa, eles geralmente não são considerados quando da criação de treinamentos desse tipo. Entretanto, os engenheiros sociais podem enganar os guardas de segurança ou outros para que eles lhes permitam a entrada em um prédio ou escritório, ou para que executem uma ação que resulte em uma invasão de computador. Embora os membros da segurança certamente não precisem do mesmo treinamento completo pelo qual passam as pessoas que operam ou usam os computadores, eles não devem ser esquecidos no programa de conscientização sobre a segurança.

Dentro do mundo corporativo talvez haja poucos assuntos sobre os quais todos os empregados precisam ser treinados e que são ao mesmo tempo tão importantes e tão aborrecidos quanto a segurança. Os melhores programas de treinamento sobre a segurança das informações devem informar e prender a atenção e o entusiasmo dos aprendizes.

O objetivo deve transformar a conscientização e o treinamento em segurança das informações em uma experiência interessante e interativa. As técnicas podem incluir a demonstração dos métodos da engenharia social por meio da dramatização, o exame de relatórios da mídia sobre ataques recentes em outras empresas com menos sorte e a discussão das maneiras pelas quais as empresas poderiam ter evitado o prejuízo. Elas também podem mostrar um vídeo sobre segurança que seja divertido e educacional ao mesmo tempo. Existem diversas empresas de conscientização sobre a segurança que comercializam vídeos e materiais relacionados.

As histórias deste livro fornecem um material rico para explicar os métodos e as táticas da engenharia social e têm o objetivo de aumentar a consciência sobre a ameaça e de demonstrar as vulnerabilidades do comportamento humano. Pense em usar os cenários aqui descritos como a base para as atividades de dramatização. As histórias também oferecem oportunidades para discussões animadas sobre como as vítimas poderiam ter respondido de forma diferente para evitar que os ataques fossem bem-sucedidos.

Um desenvolvedor habilidoso de cursos e treinadores habilidosos encontrarão muitos desafios, mas também muitas oportunidades para manter a classe interessada e. ao mesmo tempo, para motivar as pessoas a tomarem parte na solução.

A estrutura do treinamento

Um programa básico de treinamento na conscientização sobre segurança deve ser desenvolvido de modo que todos os empregados tenham de participar Os empregados novos devem participar dele

Observação

Para aquelas empresas que não têm recursos para desenvolver um programa interno, existem diversas empresas que oferecem serviços de treinamento em conscientização sobre a segurança. As feiras, tais como a Secure World Expo (www.secureworldexpo.com), são pontos onde essas empresas podem ser encontradas.

como parte de seu treinamento inicial. Recomendo que nenhum empregado receba acesso a um computador antes de ter participado de uma sessão básica de conscientização sobre a segurança.

Para essa etapa inicial, sugiro uma sessão que seja voltada para prender a atenção *e* que seja curta o suficiente para que as mensagens importantes sejam lembradas. Embora a quantidade do material abordado justifique um treinamento mais longo, a importância de fornecer a conscientização e a motivação juntamente com um número razoável de mensagens essenciais, a meu ver, é mais eficiente do que longas sessões de meio dia ou dia inteiro que deixam as pessoas tontas com tantas informações.

A ênfase dessas sessões deve estar na veiculação de uma apreciação sobre o mal que pode ser feito à empresa e aos empregados, a menos que todos tenham bons hábitos de segurança no trabalho. Mais importante do que aprender sobre as práticas específicas de segurança é a motivação que leva os empregados a aceitarem a responsabilidade pessoal pela segurança.

Em situações nas quais alguns empregados não podem participar das sessões em classe, a empresa deve pensar em desenvolver o treinamento em conscientização usando outras formas de instrução, tais como vídeos, treinamento baseado em computador, cursos on-line ou material escrito.

Após a sessão de treinamento inicial, sessões mais longas devem ser criadas para educar os empregados sobre as vulnerabilidades especificas e técnicas de ataque relativas á sua posição na empresa. Pelo menos uma vez por ano é preciso fazer um treinamento de renovação. A natureza da ameaça e os métodos usados para explorar as pessoas estão sempre mudando, de modo que o conteúdo do programa deve ser mantido atualizado. Além disso, a consciência e o preparo das pessoas diminui com o tempo, de modo que o treinamento deve se repetir a intervalos razoáveis de tempo para reforçar os princípios da segurança. Novamente a ênfase precisa estar em manter os empregados convencidos sobre a importância das políticas de segurança e motivados para que as sigam, além de expor as ameaças específicas e os métodos da engenharia social.

Os gerentes devem dar um tempo razoável a seus subordinados para que eles se familiarizem com as políticas e os procedimentos de segurança e para que participem do programa de conscientização sobre a segurança. Não se deve esperar que os empregados estudem as políticas de segurança nem participem das aulas no seu tempo vago. Os empregados novos devem ter um tempo maior para examinar as políticas de segurança e as práticas estabelecidas antes de iniciar as responsabilidades da sua função.

Os empregados que mudarem de posição dentro da organização para uma função que envolva o acesso a informações confidenciais ou sistemas de computadores devem, obviamente, fazer um programa de treinamento em segurança adaptado às suas novas responsabilidades. Por exemplo, quando um operador de computador torna-se um administrador de sistema ou quando uma recepcionista torna-se uma assistente administrativa, ambos devem passar por um novo treinamento.

Conteúdo do treinamento

Quando reduzidos às suas características fundamentais, todos os ataques da engenharia social têm o mesmo elemento comum: a fraude. A vitima é levada a acreditar que o atacante é um colega ou alguma outra pessoa que está autorizada a acessar informações confidenciais ou que está autorizada a dar à vítima instruções que envolvam a tomada de ações com um computador ou com equipamento relacionado com o computador. Quase todos esses ataques poderiam ser evitados se o empregado-alvo seguisse estas etapas:

* Verificar a identidade da pessoa que faz a solicitação: essa pessoa *é* realmente quem diz ser?

Observação

Como a conscientização e o treinamento para a segurança e o treinamento nunca são perfeitos, sempre que possível use tecnologias de segurança para aumentar seu sistema de defesa. Isso significa que a medida de segurança é fornecida pela tecnologia e não pelos empregados individuais, por exemplo, quando o sistema operacional está configurado para evitar que os empregados façam o download de software da Internet ou selecionem uma senha curta e fácil de adivinhar.

- Verificar se a pessoa está autorizada. A pessoa tem a necessidade de saber ou tem autorização para fazer a solicitação?

Se as sessões de treinamento de conscientização puderem mudar o comportamento das pessoas para que cada empregado sempre teste toda solicitação que contraria esses critérios, o risco associado aos ataques da engenharia social reduzir-se-á de modo impressionante.

Um programa prático de treinamento e conscientização sobre a segurança das informações que aborda os aspectos do comportamento humano e da engenharia social deve incluir:

- Uma descrição do modo como os atacantes usam as habilidades da engenharia social para enganar as pessoas.
- Os métodos usados pelos engenheiros sociais para atingir seus objetivos.
- Como reconhecer um provável ataque da engenharia social.
- O procedimento para o tratamento de uma solicitação suspeita.
- A quem relatar as tentativas da engenharia social ou os ataques bem-sucedidos.
- A importância de questionar todos os que fazem uma solicitação suspeita, independentemente da posição ou importância que a pessoa alega ter.
- O fato de que os funcionários não devem confiar implicitamente nas outras pessoas sem uma verificação adequada, embora o seu impulso seja dar aos outros o beneficio da dúvida.
- A importância de verificar a identidade e a autoridade de qualquer pessoa que faça uma solicitação de informações ou ação. (Consulte "Procedimentos de verificação e autorização" no Capítulo 16 para obter detalhes sobre como verificar a identidade.)
- Procedimentos para proteger as informações confidenciais, entre eles a familiaridade com todo o sistema de classificação de dados.
- A localização das políticas e dos procedimentos de segurança da empresa e a sua importância para a proteção das informações e dos sistemas de informações corporativas.
- Um resumo das principais políticas de segurança e uma explicação do seu significado. Por exemplo, cada empregado deve ser instruído sobre como criar uma senha difícil de adivinhar.
- A obrigação de cada empregado de atender às políticas e as conseqüências do seu não-atendimento.

Por definição, a engenharia social envolve algum tipo de interação humana. Com freqüência, um atacante usa vários métodos de comunicação e tecnologias para tentar atingir o seu objetivo. Por esse motivo, um programa de conscientização bem feito deve tentar abordar alguns ou todos estes itens:

- As políticas de segurança relacionadas com senhas de computador e voice mail.
- O procedimento de divulgação de informações ou material confidencial.
- A política de uso do correio eletrônico, incluindo as medidas para evitar ataques maliciosos de código, tais com vírus, worms e Cavalos de Tróia.
- Os requisitos de segurança física, tais como o uso de crachás.
- A responsabilidade de questionar as pessoas que estão nas instalações sem o crachá.
- As melhores práticas de segurança para o uso do voice mail.
- Como determinar a classificação das informações e as medidas adequadas para proteger as informações confidenciais.
- A eliminação adequada de documentos confidenciais e mídia de computador que contenham, ou que já tenham contido, material confidencial.

Da mesma forma, se a empresa pretende usar testes para determinar a eficiência das defesas contra os ataques da engenharia social, um aviso deve ser dado para que os empregados tomem conhecimento dessa prática. Deixe que saibam que em algum momento eles podem receber uma ligação telefônica ou outra comunicação que usará as técnicas do atacante como parte de tal teste. Use os resultados desses testes não para punir, mas para definir a necessidade de treinamento adicional em algumas áreas.

Os detalhes relativos a todos os itens acima podem ser encontrados no Capítulo 16.

TESTE

A sua empresa pode testar o domínio que os empregados têm das informações apresentadas no treinamento de conscientização de segurança antes de permitir o acesso ao sistema de computadores. Se os testes forem aplicados on-line, você pode usar muitos programas de projeto de avaliação que permitem analisar facilmente os resultados dos testes para determinar as áreas do treinamento que precisam ser fortalecidas.

A sua empresa também pode fornecer um certificado de conclusão do treinamento de segurança como recompensa e motivação para o empregado.

Como rotina para a conclusão do programa, recomendamos que cada empregado assine um comprometimento de seguir as políticas e os princípios de segurança que foram ministrados pelo programa. As pesquisas sugerem que uma pessoa que se compromete a assinar tal contrato tem mais chances de se esforçar para cumprir os procedimentos.

conscientização constante

A maioria das pessoas sabe que o aprendizado, mesmo das questões importantes, tende a desaparecer, a menos que seja reforçado periodicamente. Devido à importância de manter os empregados atualizados sobre o assunto da defesa contra os ataques da engenharia social, um programa constante de conscientização é de importância vital.

Um método para manter a segurança sempre na mente do empregado é fazer com que a segurança das informações seja parte específica da função de *todas* as pessoas que trabalham na empresa. Isso as encoraja a reconhecer o seu papel crucial na segurança geral da empresa. Caso contrário, há uma forte tendência de achar que a segurança "não é problema meu".

Embora a responsabilidade geral por um programa de segurança das informações normalmente seja de uma pessoa do departamento de segurança ou do departamento de tecnologia da informação, o desenvolvimento de um programa de conscientização para a segurança das informações provavelmente é mais bem estruturado como um projeto conjunto com o Departamento de Recursos Humanos.

O programa constante de conscientização precisa ser criativo e usar cada canal disponível para comunicar as mensagens de segurança para que elas sejam lembradas e para que os empregados tenham sempre em mente os bons hábitos de segurança. Os métodos devem usar todos os canais tradicionais, além dos não tradicionais que sejam imaginados pelas pessoas designadas para implementar e desenvolver o programa. Assim como acontece na propaganda tradicional, o humor e a inteligência ajudam. A mudança na redação das mensagens evita que elas se tornem familiares demais para serem ignoradas.

A lista de possibilidades de um programa constante de conscientização poderia incluir:

- O fornecimento de exemplares deste livro para todos os empregados.
- A inclusão de itens informativos nas circulares da empresa: por exemplo, artigos, lembretes (de preferência itens curtos que chamem a atenção) ou quadrinhos.
- A colocação de uma foto do Empregado da Segurança do Mês.
- Pôsteres afixados nas áreas dos empregados.
- Notas publicadas no quadro de avisos.
- O fornecimento de lembretes impressos nos envelopes de pagamento.
- O envio de lembretes por correio eletrônico.
- O uso de proteções de tela relacionadas com segurança.
- A transmissão de anúncios sobre a segurança por meio do sistema de voice mail.
- A impressão de etiquetas para o telefone com mensagens tais como "A pessoa que está ligando é quem ela diz ser?".
- A configuração de mensagens de lembrete que aparecem quando o computador é ligado, tais como "Criptografe as informações confidenciais antes de enviá-las".
- A inclusão da conscientização para a segurança como um item-padrão nos relatórios de desempenho dos empregados e nas análises anuais.
- A publicação na intranet de lembretes de conscientização para a segurança, talvez usando quadrinhos ou humor, ou alguma outra maneira que incentive as pessoas a lerem.
- O uso de um quadro eletrônico de mensagens na lanchonete, com um lembrete de segurança que seja trocado freqüentemente.
- A distribuição de folhetos ou brochuras.
- E pense naqueles biscoitos da fortuna que são distribuídos de graça na lanchonete, contendo cada um deles um lembrete sobre a segurança em vez de uma previsão.

A ameaça é constante; os lembretes também devem ser constantes.

O QUE HÁ PARA MIM?

Além dos programas de treinamento e conscientização sobre a segurança, recomendo um programa ativo e bem divulgado de recompensas. Você deve reconhecer os empregados que detectaram e evitaram uma tentativa de ataque de engenharia social ou que de alguma outra maneira contribuíram

para o sucesso do programa de segurança das informações. A existência do programa de recompensas deve ser anunciada para os empregados em todas as sessões de conscientização sobre a segurança, e as violações da segurança devem ser amplamente divulgadas em toda a organização.

Por sua vez, as pessoas devem ter conhecimento das conseqüências de não seguirem as políticas de segurança das informações por falta de cuidado ou resistência. Embora todos cometamos erros, as violações repetidas dos procedimentos de segurança não devem ser toleradas.

Capítulo 16

Recomendações de Políticas de Segurança das Informações Corporativas

Nove entre dez grandes corporações e órgãos governamentais já foram atacados por invasores de computadores, a julgar pelos resultados de uma pesquisa realizada pelo FBI e reportada pela Associated Press em abril de 2002. Curiosamente, o estudo descobriu que apenas uma em três empresas relatou ou reconheceu publicamente os ataques. Essa reserva em se confessar vítima faz sentido. Para evitar a perda da confiança do cliente e para evitar outros ataques por parte de invasores que descobriram que uma empresa pode ser vulnerável, a maioria das empresas não informa publicamente os incidentes de segurança com seus computadores.

Parece que não há estatísticas sobre os ataques da engenharia social e, se houvesse, os números seriam muito pouco confiáveis. Na maior parte dos casos uma empresa nunca sabe quando um engenheiro social "roubou" as informações, de modo que muitos ataques não são notados nem relatados.

Existem medidas efetivas que podem ser usadas contra a maioria dos tipos de ataques da engenharia social. Mas vamos enfrentar a realidade — a menos que todos da empresa entendam que a segurança é importante e façam com que seus funcionários saibam e sigam as políticas de segurança, os ataques da engenharia social sempre representarão um risco sério para a empresa.

Na verdade, a medida que os aperfeiçoamentos são feitos nas armas tecnológicas contra as quebras de segurança, a abordagem da engenharia social de usar as pessoas para acessar as informações da empresa ou penetrar na rede corporativa quase certamente serão mais freqüentes e atraentes para os ladrões das informações. Um espião industrial tentará atingir seu objetivo usando o método mais fácil e que envolva o menor risco de ser descoberto. Na verdade, uma empresa que protegeu seus sistemas de computadores e empregou tecnologias de segurança complexas pode daí para frente estar mais vulnerável aos atacantes que usam métodos e táticas da engenharia para conseguir seus objetivos.

Este capítulo apresenta as políticas específicas criadas para minimizar o risco de uma empresa sofrer ataques relacionados com engenharia social. As políticas abordam os ataques que se baseiam não apenas na exploração das vulnerabilidades técnicas, mas que envolvem o uso de algum tipo de pretexto ou truque para enganar um empregado de confiança para que ele forneça as informações relativas a determinada ação que de ao atacante o acesso às informações confidenciais da empresa ou aos seus sistemas e redes de computadores.

O QUE É UMA POLÍTICA DE SEGURANÇA?

As políticas de segurança são instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança. Essas políticas estão entre as mais significativas no que diz respeito a evitar e detectar os ataques da engenharia social.

Os controles efetivos de segurança são implementados pelo treinamento dos empregados, bem como por políticas e procedimentos bem documentados. Entretanto, é importante observar que as políticas de segurança, mesmo que sejam seguidas religiosamente por todos os empregados, não evitam todos os ataques da engenharia social. Por isso, um objetivo ideal seria sempre minimizar o risco até um nível aceitável.

As políticas apresentadas aqui incluem medidas que, embora não se concentrem estritamente nas questões da engenharia social, estão aqui porque tratam das técnicas normalmente usadas nos ataques da engenharia social. Por exemplo, as políticas sobre a abertura dos anexos de correio eletrônico — as quais podem instalar software Cavalo de Tróia, permitindo que o atacante tome o computador da vítima — abordam um método muito usado pelos invasores de computadores.

Etapas para o desenvolvimento de um programa

Um programa de segurança da informação abrangente começa com uma avaliação de risco que visa determinar:

- Quais são as informações da empresa que precisam ser protegidas?
- Quais ameaças específicas existem contra os ativos?
- Qual dano seria causado às empresas se essas ameaças em potencial se materializassem?

O objetivo primário da avaliação de risco é priorizar as informações que precisam de proteção imediata, e se essa proteção será eficaz em termos de custo com base em uma análise do custo/benefício. Em resumo, quais informações serão protegidas em primeiro lugar e quanto custará para proteger essas informações?

E essencial que a gerência de primeiro escalão adote e suporte com firmeza o desenvolvimento de políticas de segurança e de um programa de segurança das informações. Assim como qualquer outro método corporativo, para que um programa de segurança seja bem-sucedido, a gerência deve fazer mais do que apenas apoiá-lo, deve demonstrar um comprometimento pelo exemplo pessoal. Os empregados precisam ter consciência de que a gerência acredita que a segurança das informações é vital para a operação da empresa, de que a proteção das informações comerciais da empresa é essencial para que ela continue funcionando e de que o trabalho de cada empregado pode depender do sucesso do programa.

A pessoa designada para criar as políticas de segurança da informação precisa entender que as políticas devem ser escritas em um estilo que não faça uso de jargão técnico e que possa ser facilmente entendido pelo empregado não técnico. Também é importante que o documento deixe claro que cada política é importante, caso contrário os empregados podem encará-las como perda de tempo e não cumpri-las. O redator dessa política deve criar um documento que apresente as políticas e um documento separado para os procedimentos, porque as políticas provavelmente mudam com menos freqüência do que os procedimentos específicos usados para implementá-las.

Além disso, o redator das políticas deve estar consciente dos meios pelos quais as *tecnologias* da segurança podem ser usadas para implantar as boas práticas da segurança das informações. Por exemplo. a maioria dos sistemas operacionais possibilita a solicitação de que as senhas de usuário atendam a determinadas especificações, tais como tamanho. Em algumas empresas, uma política que proíbe que os usuários façam o download de programas pode ser controlada por meio de definições locais ou globais de diretrizes de segurança dentro do sistema operacional. As políticas devem exigir o uso da tecnologia sempre que isso for eficaz em termos de custo, para remover a tomada de decisão com base nas pessoas.

Os empregados devem ser aconselhados sobre as conseqüências do não-cumprimento das políticas e dos procedimentos de segurança. Um resumo das conseqüências da violação das políticas deve ser desenvolvido e amplamente divulgado. Por sua vez, um programa de recompensa deve ser criado para os empregados que demonstram boas práticas de segurança ou que reconhecem e relatam um incidente de segurança. Sempre que um empregado for recompensado por frustrar uma quebra de segurança, isso deve ser amplamente divulgado em toda a empresa, como por exemplo, em um artigo na circular da empresa.

Um dos objetivos de um programa de conscientização sobre a segurança é a comunicação da importância das políticas de segurança e o dano que a falha em seguir essas regras pode causar. Dada a natureza humana, os empregados às vezes ignoram ou sabotam as políticas que parecem ser injustificadas ou que demandam muito tempo. A gerência tem a responsabilidade de garantir que os empregados entendam a importância das políticas e sejam motivados para atendê-las, e não tratá-las como obstáculos a serem contornados.

E importante notar que as políticas de segurança das informações não podem ser inflexíveis. Uma empresa precisa mudar à medida que surgem novas tecnologias de segurança, e à medida que as vulnerabilidades de segurança evoluem, as políticas precisam ser modificadas ou suplementadas. Um processo de exame e atualização regular deve ser estabelecido. Tome as políticas e os procedimentos de segurança corporativa disponíveis por meio da intranet corporativa ou mantenha-os em uma pasta que esteja disponível para todos. Isso aumenta a probabilidade de que tais políticas e procedimentos sejam examinados com mais freqüência e fornece um método conveniente para que os empregados encontrem rapidamente a resposta para todas as perguntas relacionadas com a segurança das informações.

Finalmente, testes periódicos de penetração e avaliações de vulnerabilidade que usam os métodos e as táticas da engenharia social devem ser conduzidos para expor os pontos fracos do treinamento ou a falta de cumprimento das políticas e dos procedimentos da empresa. Antes de usar qualquer tática de teste de penetração simulado, os empregados devem ser avisados de que tais testes podem ocorrer de tempos em tempos.

Como usar essas políticas

As políticas detalhadas apresentadas neste capítulo representam apenas um subconjunto das políticas de segurança das informações que, creio, sejam necessárias para diminuir todos os riscos de segurança. Da mesma forma, as que estão incluídas aqui não devem ser consideradas como uma lista abrangente de políticas de segurança das informações. Em vez disso, elas formam a base para a criação de um corpo abrangente de políticas de segurança que sejam apropriadas para as necessidades específicas da sua empresa.

Os redatores das políticas de uma organização terão de escolher as políticas apropriadas com base no ambiente e nos objetivos de negócios de suas empresas. Cada organização, com seus requisitos de segurança diferentes, baseados nas necessidades, nos requisitos legais, na cultura organi-

zacional e nos sistemas de informações utilizados estabelecerá as políticas apresentadas e omitirá o restante.

Também é preciso fazer opções sobre a rigidez das políticas em cada categoria. Uma empresa menor localizada em uma única instalação na qual a maioria dos empregados se conhece não precisa estar muito preocupada com o fato de o atacante ligar e se fazer passar por um empregado (embora, é claro, um impostor pode se fazer passar por um fornecedor). Da mesma forma, apesar dos riscos maiores, uma empresa estruturada com uma cultura corporativa mais liberal e solta pode querer adotar apenas um subconjunto limitado das políticas recomendadas para atender a seus objetivos de segurança,

CLASSIFICAÇÃO DE DADOS

Uma política de classificação de dados é fundamental para proteger as informações de uma organização e para estabelecer as categorias responsáveis pela liberação das informações confidenciais. Essa política fornece uma estrutura para proteger as informações corporativas tornando os empregados conscientes do nível de confidencialidade de cada informação.

A operação sem uma política de classificação de dados — o que ocorre em quase todas as empresas hoje em dia — deixa a maioria dessas decisões nas mãos de funcionários individuais. As decisões dos empregados, naturalmente, baseiam-se em fatores subjetivos, e não na confidencialidade, no fator crítico e no valor das informações. As informações também são liberadas porque os empregados não têm conhecimento de que ao responder a uma solicitação de informações, eles podem estar colocando-as nas mãos de um atacante.

A política de classificação de dados define orientações para classificar as informações valiosas em vários níveis. Com uma classificação para cada item, os empregados podem acompanhar um conjunto de procedimentos de tratamento de dados que protege a empresa contra a liberação inadvertida ou descuidada das informações confidenciais. Esses procedimentos diminuem a possibilidade de que os empregados sejam enganados e revelem informações confidenciais para pessoas não autorizadas.

Cada empregado deve ser treinado na política corporativa de classificação de dados, incluindo aqueles que não usam os computadores ou os sistemas de comunicações corporativas. Como cada membro da força de trabalho corporativa — incluindo a equipe de limpeza, os guardas da segurança e a equipe da sala da copiadora, bem como consultores, contratados e até mesmo estagiários — pode ter acesso às informações confidenciais, todos podem ser um alvo de ataque.

A gerência deve designar um Proprietário das Informações que será responsável por todas as informações usadas no momento na empresa. Entre outras coisas, o Proprietário das Informações é responsável pela proteção das informações. Normalmente, o Proprietário determina o nível de classificação que será designado com base na necessidade de proteger as informações, reavalia periodicamente o nível de classificação designado e trata das alterações necessárias. O Proprietário das Informações também pode delegar a responsabilidade de proteger os dados a um *Custodiante* ou *Representante.*

Categorias e definições das classificações

As informações devem ser separadas em diversos níveis de classificação com base na sua confidencialidade. Após determinado sistema de classificação estar configurado, a reclassificação das informações em novas categorias é um processo caro e demorado. Na nossa política de exemplo escolhi quatro níveis de classificação, o que é apropriado para a maioria das empresas de médio a grande porte. Dependendo do número e dos tipos de informações confidenciais, as empresas podem optar por

incluir mais categorias para controlar mais ainda os tipos específicos de informações. Nas empresas menores, um esquema de classificação em três níveis pode ser suficiente. Lembre-se de que quanto mais complexa for a classificação, maiores serão as despesas com o treinamento dos empregados e a implantação do sistema.

Confidencial. Esta categoria de informações é a mais confidencial. As informações confidenciais só são usadas dentro da organização. Na maioria dos casos, elas só devem ser compartilhadas com um número muito limitado de pessoas que tenham necessidade absoluta de conhecê-las. A natureza das informações Confidenciais é tal que toda divulgação não autorizada pode ter um impacto sério sobre a empresa, sobre seus acionistas, seus parceiros de negócios e/ou seus clientes. Os itens das informações Confidenciais geralmente se classificam em uma destas categorias:

- As informações relativas aos segredos comerciais, o código-fonte proprietário, as especificações técnicas ou funcionais ou as informações de produto que podem ser vantajosas para um concorrente.
- As informações de marketing e financeiras não disponíveis para o público.
- Todas as outras informações que são vitais para a operação da empresa, tais como as estratégias futuras de negócios.

Particular. Esta categoria aborda as informações de natureza pessoal que se destinam apenas ao uso dentro da organização. Toda divulgação não autorizada das informações Particulares poderia ter um impacto sério sobre os empregados ou a empresa se elas fossem obtidas por pessoas não autorizadas (particularmente pelos engenheiros sociais). Os itens das informações Particulares podem incluir o histórico médico de empregados, os benefícios de saúde, as informações de contas bancárias, o histórico de salário ou qualquer outra informação pessoal identificadora que não seja de domínio público.

Observação

A categoria de informações Interna também é chamada de Confidencial pelo pessoal da segurança. Escolhi usar Interna porque o termo é auto-explicativo para o público a que se destina. Usei o termo Confidencial não como uma classificação de segurança. mas como um método conveniente de se referir às informações Confidenciais, Particulares e Internas; dito de outra forma, Confidencial refere-se a qualquer informação da empresa que não seja criada especificamente como Pública.

Interna. Esta categoria de informações pode ser fornecida livremente para todas as pessoas empregadas pela organização. Normalmente, a divulgação não autorizada das informações Internas não deve causar grandes danos para a empresa, para seus acionistas, seus parceiros de negócios, seus clientes ou seus empregados. Entretanto, as pessoas adeptas das habilidades da engenharia social podem usar essas informações para se fazerem passar por um empregado autorizado, contratado, ou fornecedor, e enganar o pessoal desavisado para que forneçam informações confidenciais, o que resultaria no acesso não autorizado aos sistemas de computadores corporativos.

Para que as informações Internas sejam divulgadas para terceiros é preciso assinar um contrato de confidencialidade. Esses terceiros incluem empregados de empresas de fornecedores, mão-de-obra contratada, empresas parceiras e assim por diante. As informações Internas incluem tudo o que seja usado durante a atividade diária de negócios e que não deve ser liberado para estranhos, tais como os gráficos organizacionais da corporação, os números de discagem de rede, os nomes dos sistemas internos, os procedimentos de acesso remoto, os códigos do centro de custo e outros.

Pública. As informações que foram criadas especificamente para liberação para o público. Este tipo de informação pode ser distribuído livremente para todas as pessoas e incluem os press releases, as informações de contato de suporte ao cliente ou as brochuras de produto. Observe que todas as informações que não são criadas especificamente como Públicas devem ser tratadas como informações Confidenciais.

Terminologia dos dados classificados

Com base nessa classificação, os dados devem ser distribuídos para determinadas categorias de pessoas. Várias políticas deste capitulo referem-se às informações que são dadas para uma *Pessoa Não Verificada.* Para fins destas políticas, uma Pessoa Não Verificada é alguém que o empregado não conhece pessoalmente, e não sabe se é um empregado ou se tem o cargo adequado para ter acesso às informações, nem se foi autorizado por terceiros.

No âmbito destas políticas, a *Pessoa de Confiança é* aquela que você conhece pessoalmente e sabe que é empregado, cliente ou consultor da empresa com o cargo adequado para ter acesso às informações. Uma Pessoa de Confiança também pode ser um empregado de outra empresa que estabeleceu um relacionamento com a sua empresa (por exemplo, um cliente, fornecedor ou parceiro estratégico de negócios que assinou um contrato de confidencialidade).

Na *autorização de terceiro,* uma Pessoa de Confiança confirma o vínculo empregatício ou status de uma pessoa e da sua autoridade para solicitar informações ou uma ação. Observe que, em alguns casos, essas políticas exigem que você verifique se a Pessoa de Confiança ainda está empregada pela empresa antes de responder a uma solicitação de informações ou ação feita por alguém para quem eles nunca deram autorização.

Uma *conta privilegiada e* um computador ou outra conta que requer permissão de acesso além da conta de usuário básica, tal como uma conta de administrador de sistema. Os empregados que tem contas privilegiadas podem modificar os privilégios de usuário ou executar as funções de sistema.

Uma *caixa de correio departamental geral* é uma caixa postal de voice mail que possui uma mensagem genérica para o departamento. Ela é usada para proteger nomes e ramais de telefone de empregados que trabalham em determinado departamento.

PROCEDIMENTOS DE VERIFICAÇÃO E AUTORIZAÇÃO

Os ladrões de informações usam táticas fraudulentas para acessar ou obter informações comerciais confidenciais ao se passar por empregados legítimos, contratados, fornecedores ou parceiros de negócios. Para manter a segurança efetiva das informações, um empregado que recebe uma solicitação para executar uma ação ou fornecer informações confidenciais deve identificar o interlocutor corretamente e verificar a sua autoridade antes de atender a uma solicitação.

Os procedimentos recomendados neste capítulo foram criados para ajudar um empregado que recebe uma solicitação por qualquer meio de comunicação, tal como telefone, correio eletrônico ou fax a determinar se a solicitação e a pessoa que a faz são legítimas.

Solicitações de uma pessoa de confiança

A solicitação de informação ou ação feita por uma Pessoa de Confiança pode exigir:

- A verificação de que a empresa emprega ou tem um relacionamento com a pessoa, e esse relacionamento prevê acesso a essa categoria de informações. Isto serve para evitar que os empregados, fornecedores, contratados e outros que não estejam mais associados à empresa façam-se passar por pessoal da ativa.
- A verificação de que a pessoa tem necessidade de saber a informação e se ela está autorizada a ter acesso às informações ou à a ação.

Solicitações de uma pessoa não verificada

Quando uma solicitação é feita por uma Pessoa Não Verificada, um processo razoável de verificação deve ser desenvolvido para checar se a pessoa que faz a solicitação está autorizada a receber as informações solicitadas, particularmente quando a solicitação envolve de alguma maneira equipamento de computador ou relacionado a ele. Este processo é um controle fundamental para evitar os ataques bem-sucedidos da engenharia social. Se estes procedimentos de verificação forem seguidos, eles reduzirão em muito os ataques da engenharia social.

É importante que você não tome o processo muito complicado a ponto de o seu custo torná-lo proibitivo, ou a ponto de os empregados o ignorarem. Como mostram as informações abaixo, o processo de verificação envolve três etapas:

- A verificação de que a pessoa é quem ela alega ser.
- A determinação de que o solicitante está empregado no momento ou compartilha de um relacionamento com a empresa no qual ele precisa ter as informações.
- A determinação de que a pessoa está autorizada a receber informações específicas ou ligar para pedir a ação.

Etapa um: verificação da identidade

As três etapas recomendadas para a verificação são relacionadas abaixo por ordem de eficiência — quanto maior o número, mais efetivo será o método. Cada item também inclui uma declaração sobre os pontos fracos daquele método em particular e o modo pelo qual um engenheiro social pode burlar os métodos e enganar o empregado.

1. ID de chamadas (supondo que este recurso esteja incluído no sistema telefônico da empresa). No visor do ID de chamadas, verifique se a ligação vem de fora ou de dentro da empresa e se o nome ou número de telefone exibido coincide com a identidade fornecida pelo interlocutor.

   Ponto fraco: As informações do ID de chamadas de uma ligação externa podem ser falsificadas por alguém que tenha acesso a um PBX ou telefone conectado ao serviço telefônico digital.

2. Ligação de retorno. Procure o nome da pessoa no diretório da empresa e ligue de volta para o ramal relacionado para verificar se o solicitante é um empregado.

   Ponto fraco: Um atacante com conhecimento suficiente pode fornecer o ramal de uma empresa para que, quando o empregado fizer a ligação de verificação para o número do telefone relacionado, a ligação seja transferida para o número de telefone externo do atacante.

3. Autorização. Uma Pessoa de Confiança que garante a identidade do solicitante e que o verifica.

   Ponto fraco: Os atacantes usam um pretexto para convencer outro empregado de que eles têm mesmo aquela identidade e, assim, podem fazer com que aquele empregado se responsabilize por eles.

4. Segredo compartilhado. Use um segredo compartilhado na empresa, tal como uma senha ou código diário.

   Ponto fraco: Se muitas pessoas compartilham do segredo, um atacante pode descobri-lo facilmente.

5. Supervisor/gerente do empregado. Ligue para o supervisor imediato do empregado e solicite a verificação.

   Ponto fraco: Se o solicitante forneceu o número do telefone do seu gerente, a pessoa com quem o empregado fala ao ligar para o número pode não ser verdadeiramente o gerente, mas sim um cúmplice do atacante.

6. E-mail seguro. Solicite uma mensagem assinada digitalmente.

   Ponto fraco: Se um atacante já comprometeu o computador de um empregado e instalou um detector de teclas digitadas *(Keystrokes loggers)* para obter a senha da chave privada do empregado, ele pode enviar um e-mail assinado digitalmente que parece ser do empregado.

7. Reconhecimento pessoal de voz. A pessoa que recebe a solicitação já falou com o solicitante (de preferência pessoalmente) e sabe com certeza que a pessoa é uma Pessoa de Confiança e está familiarizado com ela para reconhecer sua voz ao telefone.

   Ponto fraco: Este é um método relativamente seguro, o qual não pode ser burlado facilmente por um atacante, mas não tem utilidade se a pessoa que recebe a solicitação nunca falou com o solicitante.

8. Determinação dinâmica de senha. O solicitante autentica a si mesmo usando uma determinação dinâmica de senha, tal como um ID Seguro.

   Ponto fraco: Para burlar este método, um atacante teria de obter um dos dispositivos de senha dinâmica, bem como o PIN respectivo do empregado a quem o dispositivo pertence de direito, ou teria de enganar um empregado para que ele lesse as informações da tela do dispositivo e fornecesse o PIN.

9. **Pessoalmente com o ID.** O solicitante apresenta-se pessoalmente e mostra o crachá de um empregado ou outra identificação adequada, de preferência uma identificação com foto.

   Ponto fraco: Os atacantes quase sempre podem roubar o crachá de um empregado ou podem criar um crachá falso que parece ser autêntico. Entretanto, os atacantes em geral não gostam desta abordagem porque com ela correm o risco de ser identificados e detidos.

Etapa dois: verificação do status do empregado

A maior ameaça à segurança das informações não vem do engenheiro social nem do invasor habilidoso de computadores, mas de alguém muito mais próximo: o empregado que acabou de ser demitido e que busca vingança ou espera abrir seu próprio negócio usando as informações roubadas da empresa. (Observe que este procedimento também pode ser usado para verificar se alguém ainda desfruta de algum relacionamento comercial com a sua empresa, tal como um fornecedor, um consultor ou um contratado.)

Antes de fornecer as informações Confidenciais para outra pessoa ou aceitar instruções para realizar ações que envolvam computador ou equipamento relacionado, você deve verificar se o solicitante ainda é um empregado da empresa com um destes métodos:

Verificação na lista de empregados. Se a empresa tiver uma lista on-line de empregados que liste com precisão quem são os empregados ativos, verifique se o solicitante ainda está relacionado.

Verificação com o gerente do solicitante. Ligue para o gerente do solicitante usando um número de telefone relacionado no cadastro da empresa, e não um número fornecido pelo solicitante.

Verificação do departamento ou grupo de trabalho do solicitante. Ligue para o departamento ou grupo de trabalho do solicitante e verifique com alguém que trabalhe lá se o solicitante ainda é empregado da empresa.

Etapa três: verificação da necessidade de saber

Além de verificar se o solicitante é um empregado atual ou se tem um relacionamento com a sua empresa, ainda é preciso saber se ele está autorizado **a** acessar as informações solicitadas ou se está autorizado a solicitar aquelas ações específicas que afetam os computadores ou equipamento relacionado.

Essa verificação pode ser feita usando um destes métodos:

Consulte as listas de cargo/grupo de trabalho/responsabilidades. Uma empresa pode fornecer acesso fácil às informações de autorização publicando listas dos empregados que podem receber as informações. Essas listas podem estar organizadas por cargo, departamentos e grupos de trabalho, responsabilidades do empregado ou por alguma combinação desses critérios. Tais listas têm de ser mantidas on-line para que sejam atualizadas e forneçam acesso rápido às informações de autorização. Os Proprietários de Informações seriam responsáveis pela supervisão da criação e manutenção das listas que estão sob seu controle.

Observação

É importante observar que a manutenção dessas listas é um convite para o engenheiro social. Se um atacante que visa uma empresa toma conhecimento de que ela mantém tais listas, ele tem uma motivação forte para obter uma. De posse dela, ele pode abrir muitas portas e colocar a empresa em sério risco.

Obtenha autorização de um gerente. Um empregado entra em contato com o seu próprio gerente ou com o gerente do solicitante para pedir autorização para atender à solicitação.

Obtenha autorização do proprietário ou criador das informações. O Proprietário das Informações é o juiz final que determina se uma pessoa deve ou não receber o acesso. O processo para o controle do acesso baseado em computador diz que o empregado deve entrar em contato com seu gerente imediato para aprovar uma solicitação de acesso às informações levando em conta perfis de cargo existentes. Se tal perfil não existir, o gerente tem a responsabilidade de contatar o Proprietário dos Dados para pedir permissão. Essa cadeia de comandos deve ser seguida para que os Proprietários das Informações não sejam sobrecarregados com solicitações quando houver necessidade freqüente das informações.

Obtenha autorização por meio de um pacote de software proprietário. Para uma empresa grande que atua em uma indústria altamente competitiva, uma solução prática é desenvolver um pacote de software proprietário que forneça autorização de acesso às informações. Tal banco de dados armazena os nomes e os privilégios de acesso dos empregados às informações confidenciais. Os usuários não poderiam examinar os direitos de acesso de cada indivíduo, mas digitariam o nome do solicitante e o identificador associado às informações que estão sendo pedidas. Em seguida, o software fornece uma resposta indicando se **o** empregado está ou não autorizado a acessar tais informações. Essa alternativa evita o risco de criar uma lista de pessoal com os respectivos direitos de acesso a informações valiosas, criticas ou confidenciais que podem ser roubadas.

POLÍTICAS DE GERENCIAMENTO

As próximas políticas aplicam-se aos empregados no nível da gerência. Elas estão divididas em Classificação de Dados, Divulgação de Informações, Administração de Telefone e Políticas Diversas. Observe que cada categoria de política usa uma estrutura exclusiva de numeração para facilitar a identificação das políticas individuais.

Políticas de classificação de dados

A Classificação de Dados refere-se ao modo como a sua empresa classifica a confidencialidade das informações e quem deve ter acesso a elas.

1-1 Designação da classificação de dados

Política: Todas as informações valiosas, confidenciais ou críticas de negócios devem ser designadas a uma categoria de classificação pelo Proprietário das Informações ou delegado.

Explicação/Observações: O Proprietário designado ou delegado estabelece a classificação apropriada de dados para todas as informações que são usadas rotineiramente para atingir os objetivos da empresa. O Proprietário também controla quem pode acessar tais informações e sua utilização. Ele pode fazer nova designação da classificação e pode fixar um período de tempo para a desclassificação automática.

Todo outro item que não esteja marcado deve ser classificado como Confidencial.

1-2 Publicação dos procedimentos confidenciais de tratamento

Política: A empresa deve estabelecer os procedimentos que regem a liberação das informações em cada categoria.

Explicação/Observações: Depois que as classificações são feitas, devem ser estabelecidos os procedimentos para a liberação das informações pelos empregados para as pessoas fora da empresa, como detalhou o item *Procedimentos de verificação e autorização* anteriormente neste capítulo.

1-3 Rotulação de todos os itens

Política: Marque claramente o material impresso e o armazenamento de mídia que contém informações Confidenciais, Privadas ou Internas para que mostrem a classificação de dados apropriada.

Explicação/Observações: Os documentos impressos devem ter uma capa, com uma etiqueta de classificação clara, e cada página deve conter uma etiqueta de classificação que esteja visível quando o documento for aberto.

Todos os arquivos eletrônicos que não podem ser facilmente rotulados com as classificações de dados apropriadas (banco de dados ou arquivos de dados brutos) devem ser protegidos com controles de acesso para garantir que tais informações não sejam divulgadas inadequadamente, e que elas não sejam alteradas, destruídas ou acessadas.

Toda mídia de computador, tal como disquetes, fitas e CD-ROMs, deve ser rotulada com a mais alta classificação das informações que ela contém.

Divulgação das informações

A divulgação das informações envolve a liberação das informações para diversas pessoas com base em suas identidades e necessidade de obter tal informação.

2-1 Procedimento de verificação de empregado

Política: A empresa deve estabelecer procedimentos abrangentes que serão usados pelos empregados para verificar a identidade, o status e a autorização de um indivíduo antes de liberar as informações Confidenciais ou Sigilosas ou de executar uma tarefa que envolva o uso de hardware ou software de computador.

Explicação/Observações: Quando o tamanho da empresa e as necessidades de segurança justificarem, as tecnologias avançadas de segurança devem ser usadas para autenticar a identidade. A melhor prática de segurança seria o emprego de tokens de autenticação junto com um segredo compartilhado para identificar positivamente as pessoas que fazem as solicitações. Embora essa prática possa minimizar substancialmente o risco, o seu custo seria proibitivo para algumas empresas.

Nesses casos, a empresa deve usar um segredo compartilhado em toda a organização, tal como uma senha ou código diário.

2-2 Liberação das informações para terceiros

Política: Um conjunto de procedimentos recomendados de divulgação de informações deve estar disponível e todos os empregados devem ser treinados para segui-lo.

Explicação/Observações: Em geral, para os casos abaixo é preciso estabelecer procedimentos de distribuição:

- As informações disponibilizadas dentro da empresa.
- A distribuição de informações para indivíduos e empregados das organizações que têm um relacionamento estabelecido com a empresa, tal como consultores, funcionários temporários, estagiários, empregados de organizações que têm um relacionamento de fornecedor ou uma parceria estratégia com a empresa e assim por diante.
- As informações disponibilizadas fora da empresa.
- As informações de cada nível de classificação, quando estão sendo entregues em pessoa, por telefone, correio eletrônico, fax, voice mail, serviço postal, entrega de assinatura e transferência eletrônica.

2-3 Distribuição de informações confidenciais

Política: As informações confidenciais, aquelas que podem causar um dano substancial se forem obtidas por pessoas não autorizadas, podem ser entregues apenas para uma Pessoa de Confiança que tenha autorização para recebê-las.

Explicação/Observações: As informações confidenciais em uma forma física (ou seja, uma cópia impressa ou um meio de armazenamento removível) podem ser entregues:

- Pessoalmente.
- Por correio interno, fechada e marcada com a classificação Confidencial.
- Fora da empresa por um serviço de entregas conhecido (ou seja, FedEx, UPS e assim por diante) com a assinatura do destinatário, ou por um serviço postal usando uma classe de correspondência certificada ou registrada.

As informações confidenciais na forma eletrônica (arquivos de computador, arquivos de banco de dados, correio eletrônico) podem ser entregues:

- Como mensagem criptografada de correio eletrônico.
- Em um anexo de mensagem de correio eletrônico, como um arquivo criptografado.
- Por transferência eletrônica para um servidor dentro da rede interna da empresa.
- Por um programa de fax de um computador, desde que apenas os destinatários pretendidos usem a máquina de destino ou que esse destinatário esteja aguardando junto à máquina enquanto o fax está sendo enviado. Como alternativa, os documentos podem ser enviados por fax sem que o destinatário esteja presente se for enviado por um link telefônico criptografado ou para um servidor de fax protegido por senha.

As informações confidenciais podem ser discutidas pessoalmente; por telefone dentro da empresa, por telefone fora da empresa, se estiverem criptografadas, por transmissão criptografada por satélite, por link criptografado de videoconferência e por Voice Over Internet Protocol (VoIP) criptografado.

Para a transmissão por máquina de fax, o método recomendado pede que o remetente transmita uma página de rosto. Ao receber a página, o destinatário transmite uma página como resposta, demonstrando que ele está na máquina de fax. Em seguida, o remetente transmite o fax.

Os meios de comunicação a seguir não devem ser usados para discussão ou distribuição das informações Confidenciais: correio eletrônico não criptografado, mensagem de voice mail, correio regular ou qualquer método de comunicação sem fio (celular, serviço de recados ou sem fio).

2-4 Distribuição de informações particulares

Política: As informações particulares, que são aquelas sobre um ou mais empregados que, caso sejam divulgadas, podem ser usadas para causar danos a empregados ou à empresa, só podem ser entregues para uma Pessoa de Confiança que esteja autorizada a recebê-las.

Explicação/Observações: As informações particulares na forma física (ou seja, cópia impressa ou dados em um meio de armazenamento removível) podem ser entregues:

- Pessoalmente.
- Por correio interno, fechada e marcada com a classificação Particular.
- Por correio regular.

As informações particulares na forma eletrônica (arquivos de computador, arquivos de banco de dados, correio eletrônico) podem ser entregues:

- Por correio eletrônico interno.
- Por transferência eletrônica para um servidor dentro da rede interna da empresa.
- Por fax, desde que apenas o destinatário pretendido use a máquina de destino, ou que esse destinatário esteja aguardando junto à máquina de destino quando o fax for transmitido. As mensagens de fax também podem ser enviadas para servidores de fax protegidos por senha. Como alternativa, elas também podem ser enviadas sem que o destinatário esteja presente se isso for feito por um link telefônico criptografado para um servidor de fax protegido por senha.

As informações particulares podem ser discutidas pessoalmente, por telefone, em transmissão por satélite, link de videoconferência e por VoIP criptografado.

Os meios de comunicação a seguir não são aceitos para a discussão ou distribuição das informações Pa qualquer método de comunicação sem fio (celular, SMS ou sem fio).

2-5 Distribuição das informações internas

Política: As informações internas são aquelas que devem ser partilhadas apenas dentro da empresa ou com outras Pessoas de Confiança que tenham assinado um contrato de confidencialidade. Você deve estabelecer as orientações para a distribuição das informações Internas.

Explicação/Observações: As informações internas podem ser distribuídas por qualquer meio, incluindo correio eletrônico interno, mas não podem ser distribuídas fora da empresa na forma de correio eletrônico, a menos que este seja criptografado.

2-6 Discutindo informações confidenciais ao telefone

Política: Antes de liberar todas as informações que não foram designadas como Públicas pelo telefone, e necessário reconhecer pessoalmente a voz do solicitante por meio de um contato comercial prévio, ou o sistema de telefones da empresa deve identificar a ligação como sendo feita de um número de telefone interno que foi designado ao solicitante.

Explicação/Observações: Se a voz do solicitante não for conhecida, ligue para o número de telefone interno do solicitante para verificar sua voz na mensagem gravada de voice mail ou peça para o gerente do solicitante verificar a sua identidade e necessidade de ele ter as informações.

2-7 Procedimentos do pessoal do saguão ou da recepção

Política: O pessoal do saguão deve obter a identificação com foto antes de liberar qualquer pacote para qualquer pessoa que não seja conhecida como sendo um empregado da empresa. Um controle deve ser mantido para registrar o nome, o número da carteira de habilitação, a data de nascimento da pessoa, o item retirado e a data e hora em que foi retirado.

Explicação/Observações: Esta política também se aplica à transmissão de pacotes para um serviço de mensageiros ou courier, tal como FedEx, UPS ou Airborne Express. Essas empresas emitem cartões de identificação que podem ser usados para verificar a identidade do empregado.

2-8 Transferência de software para terceiros

Política: Antes da transferência ou divulgação de qualquer software, programa ou instruções de computador, a identidade do solicitante deve ser verificada positivamente e e preciso estabelecer se tal liberação está de acordo com a classificação de dados designada a tais informações. Normalmente, o software desenvolvido in house no formato de código-fonte é considerado altamente proprietário e classificado como Confidencial.

Explicação/Observações: A determinação da autorização geralmente se baseia no fato de o solicitante precisar acessar o software para realizar seu trabalho.

2-9 Qualificação de vendas e marketing das pistas de clientes

Política: O pessoal de vendas e marketing deve qualificar as pistas antes de liberar os números internos de callback, os planos de produto, os contatos do grupo de produto ou outras informações Sigilosas para um cliente em potencial.

Explicação/Observações: Uma tática comum dos espiões industriais é entrar em contato com um representante de vendas e marketing e fazer com que ele acredite que uma grande compra está para ser feita. Em um esforço para aproveitar a oportunidade de vendas, os representantes de vendas e marketing quase sempre liberam as informações que podem ser usadas pelo atacante como uma ficha de pôquer para obter o acesso às informações Sigilosas.

2-10 Transferência de arquivos ou dados

Política: Os arquivos ou outros dados eletrônicos não devem ser transferidos para nenhuma mídia removível, a menos que o solicitante seja uma Pessoa de Confiança cuja identidade tenha sido verificada e que tenha a necessidade de ter tais dados naquele formato.

Explicação/Observações: Um engenheiro social pode enganar facilmente um empregado fornecendo uma solicitação plausível para que as informações Sigilosas sejam copiadas para uma fita, disco de zip ou outra mídia removível e para que elas sejam enviadas para ele ou mantidas na recepção para retirada.

Administração de telefone

As políticas de administração do telefone garantem que os empregados possam verificar a identidade do interlocutor e protegem suas próprias informações de contato contra aqueles que ligam para a empresa.

3-1 Encaminhamento de chamadas nos números de discagem ou fax

Política: Os serviços que permitem o encaminhamento das chamadas para números de telefones externos não devem ser realizados em qualquer modem de discagem ou número de telefone de fax dentro da empresa.

Explicação/Observações: Os atacantes sofisticados podem tentar enganar o pessoal ou os funcionários internos da empresa de telefonia para que eles encaminhem os números internos para uma linha telefônica externa sob o controle de um atacante. Esse ataque permite que o intruso intercepte faxes, solicite que informações Confidenciais sejam enviadas por fax dentro da empresa (o pessoal supõe que o envio de mensagens de fax dentro da organização seja seguro) ou engane os usuários de discagem para que forneçam suas senhas de conta para o encaminhamento das linhas de discagem para um computador falso que simula o processo de login.

Dependendo do serviço telefônico usado dentro da empresa, o recurso de encaminhamento de chamadas pode estar sob o controle do provedor de comunicações, e não sob o controle do departamento de telecomunicações. Em tais circunstâncias, uma solicitação será feita para o provedor de comunicações para garantir que esse recurso não esteja presente nos números de telefone designados para as linhas de discagem e fax.

3-2 ID de chamadas

Política: O sistema telefônico corporativo deve fornecer a identificação da linha do interlocutor (ID de chamadas) em todos os aparelhos internos de telefone e, se possível, deve permitir um toque distinto para indicar quando uma ligação é feita de fora da empresa.

Explicação/Observações: Se os empregados puderem verificar a identidade das ligações telefônicas de fora da empresa, podem impedir um ataque ou podem encaminhar o atacante para o pessoal adequado na segurança.

3-3 Telefones de cortesia

Política: Para evitar que os visitantes façam-se passar por funcionários da empresa, cada telefone de cortesia indicará claramente a localização da chamada (por exemplo, "Saguão") no ID de chamadas do destinatário.

Explicação/Observações: Se o ID de chamadas internas mostrar apenas um número de ramal, as medidas apropriadas devem ser tomadas para as ligações feitas dos telefones da empresa na área de recepção e em todas as outras áreas públicas. Um atacante não pode conseguir fazer uma ligação de um desses telefones e enganar um empregado para que ele acredite que a ligação foi feita internamente de um telefone da empresa.

3-4 Senhas default do fabricante enviadas com os sistemas de telefone

Política: O administrador do voice mail deve alterar todas as senhas default que vieram com o sistema de telefonia antes de ele ser usado pelo pessoal da empresa.

Explicação/Observações: Os engenheiros sociais podem obter as listas das senhas default com os fabricantes e podem usá-las para acessar as contas de administrador.

3-5 Caixas postais de departamento

Política: Configure uma caixa postal de voz genérica para cada departamento que normalmente tenha contato com o público.

Explicação/Observações: A primeira etapa da engenharia social envolve a coleta das informações sobre a empresa-alvo e seu pessoal. Limitando a acessibilidade dos nomes e números de telefone dos empregados, uma empresa torna mais difícil para o engenheiro social a identificação dos alvos ou a obtenção dos nomes dos empregados legítimos que são usados para enganar o outro pessoal.

3-6 Verificação do fabricante do sistema de telefones

Política: Nenhum técnico do suporte do fabricante poderá acessar remotamente o sistema de telefones da empresa sem a identificação positiva do fabricante e a autorização para executar tal trabalho.

Explicação/Observações: Os intrusos de computadores que têm acesso aos sistemas telefônicos corporativos ganham a capacidade de criar caixas postais de voz, de interceptar as mensagens destinadas a outros usuários ou de fazer ligações telefônicas grátis pagas pela corporação.

3-7 Configuração do sistema de telefones

Política: O administrador do sistema de voice mail implantará os requisitos de segurança configurando os parâmetros de segurança adequados no sistema de telefones.

Explicação/Observações: Os sistemas de telefones podem ser configurados com níveis de segurança maiores ou menores para as mensagens de voice mail. O administrador deve ter consciência das questões de segurança da empresa e deve trabalhar com o pessoal da segurança para configurar o sistema de telefones para proteger os dados Sigilosos.

3-8 Recurso de rastreamento de chamadas

Política: Dependendo das limitações do provedor de comunicações, o recurso de rastreamento de chamadas será ativado globalmente para permitir que os empregados ativem esse recurso quando suspeitarem que o interlocutor é um atacante.

Explicação/Observações: Os empregados devem ser treinados no uso do rastreamento de chamadas e nas circunstâncias apropriadas em que ele deve ser usado. Isso pode ser feito quando o interlocutor está tentando um acesso não autorizado aos sistemas corporativos de computadores ou está solicitando informações Sigilosas. Sempre que um empregado ativa o recurso de rastreamento de chamada, uma notificação imediata deve ser enviada para o Grupo de Relatório de Incidentes.

3-9 Sistemas automatizados de telefones

Política: Se a empresa usa um sistema de resposta automatizada de telefone, o sistema deve ser programado para que os ramais de telefone não sejam anunciados quando se transfere uma ligação para um empregado ou departamento.

Explicação/Observações: Os atacantes podem usar o sistema automatizado de telefones de uma empresa para mapear os nomes e as extensões dos empregados. Em seguida, podem usar o conhecimento dessas extensões para convencer os destinatários das ligações que eles são empregados e têm direito de obter as informações internas.

3-10 Caixas postais de voz que são desativadas após sucessivas tentativas inválidas de acesso

Política: Programe o sistema corporativo de telefones para bloquear toda conta de voice mail sempre que um número especificado de tentativas inválidas de acesso tenha sido feito.

Explicação/Observações: O administrador de Telecomunicações deve bloquear uma caixa postal de voz após cinco tentativas inválidas e sucessivas de login. Em seguida, deve redefinir manualmente todos os bloqueios do voice mail.

3-11 Ramais de telefone restritos

Política: Todos os ramais internos de telefone de departamentos ou grupos de trabalho que normalmente não recebem ligações externas (help desk, sala de computadores, suporte técnico do empregado e outros) devem ser programados para que só sejam acessados dos ramais internos. Como alternativa, podem ser protegidos com senhas para que os empregados e outras pessoas autorizadas que ligam de fora saibam a senha correta.

Explicação/Observações: Embora o uso desta política bloqueie a maioria das tentativas de engenheiros sociais amadores de atingir seus prováveis alvos, *é* preciso notar que um determinado atacante às vezes pode convencer um empregado a ligar para o ramal restrito e pedir para a pessoa que atender para que ela ligue para o atacante, ou simplesmente falar no ramal restrito. Durante o treinamento de segurança, esse método de enganar os empregados para que eles ajudem o intruso deve ser discutido para que o empregado tenha conhecimento dessas táticas.

Políticas Diversas

4-1 Projeto do crachá do empregado

Política: Os crachás dos empregados devem ser criados para incluir uma foto grande que possa ser reconhecida à distância.

Explicação/Observações: A fotografia comum dos crachás de identificação corporativa só é, para fins de segurança, ligeiramente melhor do que nada. A distância entre uma pessoa que entra no prédio e o guarda ou recepcionista que tem a responsabilidade de verificar a identificação em geral é grande, e se a foto for muito pequena, não será reconhecida quando a pessoa passar Para que a foto tenha valor nessa situação, o crachá precisa ser reprojetado.

4-2 Exame dos direitos de acesso quando há mudança de posição ou responsabilidade

Política: Sempre que um empregado da empresa muda de posição ou recebe responsabilidades maiores ou menores, o gerente do empregado notificará o departamento de TI sobre a mudança nas responsabilidades do empregado para que o perfil de segurança apropriado possa ser designado.

Explicação/Observações: O gerenciamento dos direitos de acesso do pessoal é necessário para limitar a divulgação das informações protegidas. A regra do *menor privilégio* será aplicada. Os direitos de acesso designados aos usuários serão o mínimo necessário para executar suas tarefas. Todas as solicitações de mudanças que resultem em direitos de acesso mais altos devem estar de acordo com uma política para conceder direitos de acesso elevados.

O gerente do funcionário ou o departamento de recursos humanos terá a responsabilidade de notificar o departamento de tecnologia da informação para que ele ajuste os direitos de acesso do dono da conta.

4-3 Identificação especial para não-empregados

Política: A sua empresa deve emitir um crachá especial com foto para o pessoal de entrega de confiança e para não-empregados que tenham a necessidade comercial de entrar nas instalações da empresa regularmente.

Explicação/Observações: Os não-empregados que precisam entrar no prédio regularmente (por exemplo, para fazer entrega de alimentos ou bebidas para o refeitório ou para consertar as máquinas copiadoras ou fazer instalações telefônicas) podem significar uma ameaça para a sua empresa. Além de emitir identificação para esses visitantes, verifique se os seus empregados estão treinados para detectar um visitante sem crachá e se sabem como agir nessa situação.

4-4 Desativando as contas de computador dos contratados

Política: Sempre que um contratado que tenha recebido uma conta de computador conclui a sua função ou quando o contrato expira, o gerente responsável notificará imediatamente o departamento de tecnologia da informação para que eles desativem as contas de computador do contratado, incluindo todas as contas usadas para o acesso a bancos de dados, discagem ou o acesso à Internet de localizações remotas.

Explicação/Observações: Quando o contrato de trabalho de um funcionário termina, sempre há o perigo de que ele use o conhecimento dos sistemas e procedimentos da empresa para ter acesso aos dados. Todas as contas de computador usadas ou de conhecimento do funcionário devem ser prontamente desativadas. Isso inclui as contas que fornecem o acesso aos bancos de dados de produção, às contas de discagem remota e a todas as contas usadas para acessar os dispositivos relacionados com computadores.

4-5 Organização do relatório de incidentes

Política: Uma organização de relatório de incidentes deve ser estabelecida ou, nas empresas menores, uma pessoa e um substituto encarregados do relatório de incidentes devem ser designados para receber e distribuir os alertas relativos a possíveis incidentes de segurança em andamento.

Explicação/Observações: Centralizando o relatório de incidentes suspeitos de segurança, um ataque que possa ter passado despercebido pode ser detectado. No caso de ataques sistemáticos em toda a organização serem detectados e relatados, a organização de relatório de incidentes pode determinar o que o atacante está visando para que medidas especiais sejam tomadas para proteger aqueles ativos.

Os empregados designados para receber os relatórios de incidentes devem se familiarizar com os métodos e as táticas da engenharia social para que avaliem os relatórios e reconheçam quando um ataque pode estar em andamento.

4-6 Linha exclusiva de relatório de incidentes

Política: Deve ser estabelecida uma linha exclusiva para a organização de relatório de incidentes, que pode ser um ramal telefônico fácil de lembrar.

Explicação/Observações: Quando os empregados suspeitarem de que são alvos de um ataque da engenharia social, devem poder notificar imediatamente a organização de relatório de incidentes. Para que a notificação seja eficaz, todos os telefonistas e recepcionistas da empresa devem ter o número à mão ou imediatamente disponível.

Um sistema de avisos em toda a empresa pode auxiliar muito a organização na detecção e resposta a um ataque em andamento. Os empregados devem ser bem treinados para que, ao suspeitarem de que foram alvo de um ataque da engenharia social, eles imediatamente liguem para a linha exclusiva de relatório de incidentes. De acordo com os procedimentos publicados, o pessoal do relatório de incidentes notificará imediatamente os grupos-alvo para o fato de que uma intrusão pode estar em andamento e para que o pessoal fique alerta. Para que a notificação seja eficaz, o número exclusivo de relatório deve ser distribuído em toda a empresa.

4-7 As áreas sigilosas devem estar seguras

Política: Um guarda de segurança examinará o acesso às áreas sigilosas ou seguras e deve exigir duas formas de autenticação.

Explicação/Observações: Uma forma aceitável de autenticação usa um sistema eletrônico digital que requer que o empregado passe o seu crachá e digite um código de acesso. O melhor método para dar segurança às áreas sigilosas é colocar um guarda da segurança que observa toda a entrada de acesso controlado. Nas organizações em que isso fica muito caro, duas formas de autenticação devem ser usadas para validar a identidade. Dependendo do risco e do custo, um cartão de acesso com um sistema biométrico é recomendado.

4-8 Centrais de rede e telefonia

Política: Os gabinetes, armários ou salas que contêm cabeamento de rede, fiação de telefone ou pontos de acesso de rede devem estar sempre seguros.

Explicação/Observações: Apenas o pessoal autorizado terá permissão de acesso aos gabinetes, salas ou armários de telefones. Todo o pessoal da manutenção externa ou o pessoal do fabricante deve ser identificado de forma positiva usando os procedimentos publicados pelo departamento responsável pela segurança das informações. O acesso às linhas telefônicas, aos hubs de rede, chaves, PBX, bridges ou outro equipamento relacionado pode ser usado por um atacante para comprometer a segurança dos computadores e da rede.

4-9 Caixas de correio entre empresas

Política: As caixas de correio entre empresas não devem estar localizadas nas áreas acessíveis ao público.

Explicação/Observações: Os espiões industriais ou os intrusos de computador que têm acesso aos pontos de coleta de correspondência entre as empresas podem facilmente enviar cartas de autorização ou formulários internos falsos que autorizam o pessoal a liberar as informações Confidenciais ou a executar uma ação que auxilie o atacante. Além disso, o atacante pode enviar um disquete ou mídia eletrônica com instruções para a instalação de uma atualização de software ou pode abrir um arquivo que tenha comandos de macro incorporados, que servem aos objetivos do intruso. Naturalmente, quem recebe supõe que toda solicitação enviada pelo correio entre empresas seja autêntica.

4-10 O quadro de avisos da empresa

Política: Para beneficio dos funcionários da empresa, os quadros de aviso não devem estar localizados nas dependências às quais o público tenha acesso.

Explicação/Observações: Muitas empresas têm quadros de aviso nos quais as informações particulares da empresa ou do pessoal são publicadas para que todos possam ler. Os avisos do empregados, as listas de empregados, os memorandos internos, os números de contato residencial dos empregados relacionados nos anúncios e outras informações semelhantes freqüentemente são colocadas no quadro.

Os quadros de avisos podem estar localizados próximo aos refeitórios da empresa ou perto das áreas de fumantes ou de descanso às quais os visitantes têm livre acesso. Esse tipo de informação não deve ser disponibilizado para os visitantes ou o público.

4-11 Entrada no centro de computadores

Política: A sala de computadores ou o centro de dados devem estar sempre trancados e o pessoal deve autenticar a sua identidade antes de entrar.

Explicação/Observações: A segurança corporativa deve levar em conta o emprego de um crachá eletrônico ou um leitor de cartão de acesso para que todas as entradas possam ser registradas e auditadas eletronicamente.

4-12 Contas de clientes com provedores de serviços

Política: O pessoal da empresa que fez pedidos de serviços para fornecedores de serviços críticos para a empresa deve configurar uma senha de conta para evitar que as pessoas não autorizadas façam pedidos em nome da empresa.

Explicação/Observações: As empresas de serviços públicos e muitos outros fornecedores permitem que os clientes configurem uma senha sob pedido; a empresa deve estabelecer as senhas com todos os fabricantes que fornecem serviços importantes. Essa política é particularmente necessária para as telecomunicações e os serviços da Internet. Como todos os serviços de tempo critico podem ser afetados, uma senha secreta é necessária para verificar se o interlocutor está autorizado a fazer esses pedidos. Observe também que não devem ser usados identificadores, tais como o número do seguro social, o número de identificação de contribuinte na Receita Federal, o nome de solteira da mãe ou outros identificadores semelhantes.

Um engenheiro social pode, por exemplo, ligar para a empresa de telefonia e fazer pedidos para a inclusão de recursos, tais como o encaminhamento de chamadas para linhas de modem por discagem, ou pode fazer uma solicitação ao provedor de serviços da Internet para mudar as informações de conversão para fornecer um endereço IP falso quando os usuários executarem uma pesquisa de nome de host.

4-1 3 Pessoal de contato no departamento

Política: A sua empresa pode instituir um programa no qual cada departamento ou grupo de trabalho designa a um empregado a responsabilidade de agir como um ponto de contato para que todo o pessoal possa facilmente verificar a identidade das pessoas desconhecidas que alegam ser daquele departamento. Por exemplo, o help desk pode entrar em contato com essa pessoa para verificar a identidade de um empregado que está solicitando suporte.

Explicação/Observações: Este método de verificação da identidade reduz o conjunto de empregados que estão autorizados a certificar os empregados dentro de seus departamentos quando solicitam suporte tal como a redefinição de senhas ou outras questões relacionadas com contas.

Em parte, os ataques da engenharia social são bem-sucedidos porque o pessoal do suporte técnico sofre pressões de tempo e não verifica a identidade dos solicitantes. Em geral, a equipe de suporte não pode reconhecer pessoalmente todo o pessoal autorizado devido ao número de empregados das organizações maiores. Ter um empregado responsável pela identificação em cada departamento limita o número de empregados que a equipe de suporte técnica precisa conhecer pessoalmente para fins de verificação.

4-14 Senhas de cliente

Política: Os representantes do serviço ao cliente não devem poder recuperar as senhas de conta dos clientes.

Explicação/Observações: Os engenheiros sociais freqüentemente ligam para os departamentos de serviço ao cliente e, com algum pretexto, tentam obter as informações de autenticação de um cliente, tal como a senha ou o número do seguro social. Com essas informações, o engenheiro social pode ligar para outro representante do serviço, fingir que é o cliente e obter as informações ou fazer pedidos fraudulentos.

Para evitar que essas tentativas sejam bem-sucedidas, o software do serviço ao cliente deve ser criado para que os representantes só possam digitar as informações de autenticação fornecidas pelo interlocutor e recebam uma resposta do sistema indicando se a senha está ou não correta.

4-1 5 Teste de vulnerabilidade

Política: A notificação de que a empresa está usando táticas para testar as vulnerabilidades de segurança é necessária durante o treinamento de conscientização da segurança e orientação dos empregados.

Explicação/Observações: Sem a notificação do teste de penetração da engenharia social, o pessoal da empresa pode sofrer constrangimentos, pode ficar com raiva ou ter outro trauma emocional com o uso das táticas simuladas usadas contra eles por outros empregados ou contratados. Avisando os funcionários durante o processo de orientação de que eles podem estar sujeitos a esse teste você evita tal conflito.

4-16 Exibição das informações Confidenciais da empresa

Política: As informações da empresa que não foram criadas para a liberação externa não devem ser exibidas em nenhuma das áreas acessíveis do público.

Explicação/Observações: Além das informações Confidenciais de produto ou procedimento, as informações internas de contato, tais como as listas internas de telefones ou empregados, ou as listagens do prédio que contêm uma lista do pessoal da gerência de cada departamento da empresa também devem ser mantidas fora da visão de todos.

4-1 7 O treinamento de conscientização em segurança

Política: Todas as pessoas empregadas pela empresa devem concluir um curso de treinamento em conscientização da segurança. Além disso, cada funcionário deve fazer um curso de atualização sobre conscientização de segurança em intervalos regulares, os quais não podem exceder 12 meses, conforme requisito do departamento que tem a responsabilidade do treinamento em segurança.

Explicação/Observações: Muitas organizações ignoram o treinamento de conscientização em segurança. De acordo com a Pesquisa da Segurança das Informações Globais de 2001, apenas 30% das organizações pesquisadas gastam dinheiro em treinamento de conscientização para a sua comunidade de usuários. O treinamento em conscientização é um requisito essencial para diminuir as quebras de segurança bem-sucedidas que utilizam técnicas da engenharia social.

4-1 8 Curso de treinamento em segurança para o acesso ao computador

Política: O pessoal deve participar de um curso de informações de segurança e concluí-lo antes de ter acesso a qualquer sistema de computador da empresa.

Explicação/Observações: Os engenheiros sociais com freqüência visam aos empregados novos, sabendo que, como um grupo em geral, eles são as pessoas com menos chances de estar cientes das políticas de segurança da empresa e dos procedimentos adequados para determinar a classificação e o tratamento das informações sigilosas.

O treinamento deve incluir uma oportunidade para que os empregados façam perguntas sobre as políticas de segurança. Após o treinamento, o dono da conta deve assinar um documento reconhecendo a sua compreensão das políticas de segurança e a sua concordância em segui-las.

4-1 9 O crachá do empregado deve ser codificado com cores

Política: Os crachás de identificação devem ser codificados com cores para indicar se o portador é um empregado, contratado, temporário, fornecedor, consultor, visitante ou estagiário.

Explicação/Observações: A cor do crachá é um modo excelente de determinar o status de uma pessoa à distância. Uma alternativa seria usar letras grandes para indicar o status do portador, mas o uso de um esquema de código de cores é inconfundível e mais fácil de ser visto.

Uma tática comum da engenharia social para obter o acesso físico a um prédio é vestir-se como um entregador ou técnico. Uma vez dentro da instalação, o atacante faz-se passar por outro empregado ou mente sobre o seu status para obter a cooperação dos demais. A finalidade desta política é evitar que as pessoas entrem no prédio legitimamente e, em seguida, entrem nas áreas às quais não deveriam ter acesso. Por exemplo, uma pessoa que entra na instalação como um técnico da empresa de telefonia não poderia se fazer passar por um empregado. A cor do crachá o denunciaria.

POLÍTICAS DA TECNOLOGIA DA INFORMAÇÃO

O departamento de tecnologia da informação de qualquer empresa deve ter um conjunto especial de políticas que o ajude a proteger os ativos de informações da organização. Para refletir a estrutura típica das operações de TI de uma organização, dividi as políticas de TI em Geral, Help Desk, Administração de Computadores e Operações de Computadores.

Geral

5-1 Informações de contato dos funcionários do departamento de TI

Política: Os números de telefone e os endereços de correio eletrônico dos funcionários do departamento de TI não devem ser divulgados para nenhuma pessoa que não tenha necessidade dessas informações.

Explicação/Observações: A finalidade desta política é evitar que essas informações sejam usadas pelos engenheiros sociais. Ao divulgar apenas um número geral de contato ou endereço de correio eletrônico, as pessoas de fora da empresa ficam impedidas de entrar diretamente em contato com o pessoal de TI. Os endereços de correio eletrônicos dos contatos técnicos e administrativos do site só devem consistir em nomes genéricos, tais como admin@companyname.com; os números de telefone publicados devem conectar-se a uma caixa postal departamental, não aos funcionários individuais.

Quando as informações para contato direto estão disponíveis, um intruso pode acessar facilmente os funcionários específicos de TI e enganá-los para que eles forneçam informações que podem ser usadas em um ataque, ou para fazerem-se passar pelos empregados de TI usando seus nomes e suas informações de contato.

5-2 Solicitações de suporte técnico

Política: Todas as solicitações de suporte técnico devem ser enviadas para o grupo que trata de tais solicitações.

Explicação/Observações: Os engenheiros sociais podem tentar visar o pessoal de TI que não trata normalmente das questões de suporte técnico e que talvez não esteja a par dos procedimen-

tos de segurança adequados ao lidar com tais solicitações. Da mesma forma, a equipe de TI deve ser treinada para negar essas solicitações e enviar o interlocutor para o grupo que tem a responsabilidade de fornecer o suporte.

Help Desk

6-1 Procedimentos de acesso remoto

Política: O pessoal do help desk não deve divulgar detalhes ou instruções relativos ao acesso remoto, entre elas os pontos de acesso externos da rede ou os números de discagem, a menos que o solicitante lenha sido:

- Verificado como autorizado a receber as informações Internas e
- Verificado como autorizado para se conectar à rede corporativa como um usuário externo. A menos que seja pessoalmente conhecido, o solicitante deve ser identificado positivamente de acordo com os Procedimentos de Verificação e Autorização destacados no início deste capítulo.

Explicação/Observações: O help desk corporativo quase sempre é o alvo principal do engenheiro social, seja porque a natureza do seu trabalho é auxiliar os usuários nas questões relacionadas com computadores, seja porque eles geralmente têm privilégios de sistema altos. Todo o pessoal do help desk deve ser treinado para agir como um firewall humano para evitar a divulgação não autorizada das informações que ajudarão qualquer pessoa não autorizada a ter acesso aos recursos da empresa. A regra simples é nunca divulgar os procedimentos de acesso remoto a ninguém que não tenha uma verificação positiva da identidade.

6-2 Redefinindo as senhas

Política: A senha para uma conta de usuário só pode ser redefinida sob solicitação do dono da conta.

Explicação/Observações: O truque mais usado pelos engenheiros sociais é fazer com que a senha da conta de outra pessoa seja redefinida ou alterada. O atacante faz-se passar pelo empregado usando o pretexto de que sua senha foi perdida ou esquecida. Em um esforço para reduzir o sucesso desse tipo de ataque, um empregado de TI que recebe uma solicitação de mudança de senha deve ligar de volta para o empregado antes de fazer qualquer coisa. Essa ligação não deve ser feita para um número de telefone fornecido pelo solicitante, mas para um número obtido na lista de telefones de empregados. Consulte os Procedimentos de Verificação e Autorização para saber mais sobre esse procedimento.

6-3 Alterando os privilégios de acesso

Política: Todas as solicitações para aumentar os privilégios ou direitos de acesso de um usuário devem ser aprovadas por escrito pelo gerente do dono da conta. Quando a alteração for feita, uma confirmação deve ser enviada para o gerente do solicitando pelo correio interno da empresa. Além disso, tais solicitações devem ser verificadas como autênticas de acordo com os Procedimentos de Verificação e Autorização.

Explicação/Observações: Depois que um intruso de computador comprometeu uma conta de usuário padrão, a próxima etapa é aumentar seus privilégios para que ele tenha o controle completo do sistema comprometido. Um atacante que tem conhecimento do processo de autorização pode forjar uma solicitação autorizada quando forem usados correio eletrônico, fax ou telefone para transmiti-la. Por exemplo, ele pode ligar para o suporte técnico ou o help desk e tentar convencer um técnico a conceder direitos de acesso adicionais para a conta comprometida.

6-4 Nova autorização de conta

Política: Quando for preciso criar uma conta nova para um empregado, contratado ou outra pessoa autorizada, essa solicitação deve ser feita por escrito e assinada pelo gerente do empregado, ou enviada por correio eletrônico assinado digitalmente. Essas solicitações também devem ser verificadas pelo envio de uma confirmação de solicitação por meio do correio interno da empresa.

Explicação/Observações: Como as senhas e outras informações úteis para entrar nos sistemas de computadores são os alvos de prioridade mais alta para os ladrões de informações, medidas especiais precisam ser tomadas. A intenção desta política é evitar que os intrusos façam-se passar por pessoal autorizado para forjar solicitações de novas contas. Assim sendo, todas essas solicitações devem ser verificadas positivamente usando os Procedimentos de Verificação e Autorização.

6-5 Entrega de senhas novas

Política: As senhas novas devem ser tratadas como informações Confidenciais da empresa e devem ser entregues por métodos seguros, seja pessoalmente ou por um serviço de entrega com confirmação, tal como correio registrado ou por UPS ou FedEx. Consulte as políticas de distribuição das informações Confidenciais.

Explicação/Observações: O correio interno da empresa também pode ser usado, mas recomenda-se que as senhas sejam enviadas em envelopes seguros que escondam o conteúdo. Um método sugerido é estabelecer uma pessoa que cuide dos computadores em cada departamento, a qual tenha a responsabilidade de lidar com a distribuição dos detalhes da conta nova e a confirmação da identidade do pessoal que perde ou se esquece de suas senhas. Nessas circunstâncias. o pessoal de suporte sempre estaria trabalhando com um grupo menor de empregados que seria reconhecido pessoalmente.

6-6 Desativando uma conta

Política: Antes de desativar a conta de um usuário você deve confirmar se a solicitação foi feita pelo pessoal autorizado.

Explicação/Observações: A intenção desta política e evitar que um atacante crie uma solicitação para desativar uma conta e, em seguida, ligue para solucionar os problemas da incapacidade do usuário em acessar o sistema de computadores. Quando o engenheiro social liga fazendo-se passar por um técnico com conhecimento da inabilidade do usuário em fazer o login, a vitima quase sempre concorda com uma solicitação para revelar a sua senha durante o processo de solução de problemas.

6-7 Desativando as portas ou os dispositivos de rede

Política: Nenhum empregado deve desativar nenhum dispositivo ou porta de rede para pessoal não verificado do suporte técnico.

Explicação/Observações: A intenção desta política é evitar que um atacante crie uma solicitação para desativar uma porta de rede e, em seguida, ligue para o funcionário para solucionar a sua incapacidade de acessar a rede.

Quando o engenheiro social que se faz passar por um técnico liga e demonstra já ter conhecimento do problema de rede do usuário, a vítima quase sempre concorda com uma solicitação de revelar a sua senha durante o processo de solução do problema.

6-8 Divulgação dos procedimentos para o acesso sem fio

Política: Nenhum funcionário deve divulgar os procedimentos para acessar os sistemas da empresa nas redes sem fio para qualquer pessoa que não esteja autorizada a se conectar com a rede sem fio.

Explicação/Observações: Sempre confirme se o solicitante é uma pessoa autorizada a se conectar à rede corporativa como usuário externo antes de liberar as informações de acesso sem fio. Consulte os Procedimentos de Verificação e Autorização.

6-9 Nome dos usuários com problemas

Política: Os nomes dos empregados que relataram problemas relacionados com computadores não devem ser revelados fora do departamento de tecnologia da informação.

Explicação/Observações: Em um ataque típico, um engenheiro social liga para o help desk e solicita os nomes dos funcionários que relataram problemas recentes com o computador. O interlocutor pode se fazer passar por um funcionário, fornecedor ou um empregado da empresa de telefonia. Depois de obter os nomes dessas pessoas, o engenheiro social faz-se passar por uma pessoa do help desk ou suporte técnico, entra em contato com o empregado e diz que está ligando para solucionar o problema. Durante a ligação, o atacante faz a vítima fornecer as informações desejadas ou executar uma ação que facilita o objetivo do atacante.

6-10 Iniciando comandos de execução ou executando programas

Política: O pessoal empregado no departamento de TI que tem contas privilegiadas não deve executar nenhum comando ou programa de aplicativo sob solicitação de qualquer pessoa que eles não conheçam pessoalmente.

Explicação/Observações: Um método comum usado pelos atacantes para instalar um programa de Cavalo de Tróia ou outro software malicioso é mudar o nome de um programa existente e, em seguida, ligar para o help desk reclamando que uma mensagem de erro aparece sempre que uma tentativa é feita para executar o programa. O atacante convence o técnico do help desk a executar o programa ele mesmo. Quando o técnico atende ao pedido, o software malicioso herda os privilégios do usuário que executa o programa e executa uma tarefa, a qual dá ao atacante os mesmos privilégios sobre o computador do empregado do help desk. Isso permite que o atacante assuma o controle do sistema da empresa.

Esta política visa combater essa tática ao exigir que o pessoal do suporte verifique o status de emprego antes de executar qualquer programa sob solicitação de um interlocutor.

Administração de computadores

7-1 Alterando os direitos de acesso globais

Política: Uma solicitação para alterar os direitos de acesso globais associados a um perfil eletrônico de cargo deve ser aprovada pelo grupo que tem a responsabilidade de gerenciar os direitos de acesso à rede corporativa.

Explicação/Observações: O pessoal autorizado analisará cada uma dessas solicitações para determinar se a alteração pode criar uma ameaça à segurança das informações. Nesse caso, o empregado responsável cuidará dos problemas pertinentes com o solicitante para chegar conjuntamente a uma decisão sobre as alterações a serem feitas.

7-2 Solicitações de acesso remoto

Política: O acesso remoto ao computador só será fornecido para o pessoal que demonstrou a necessidade de acessar os sistemas corporativos da empresa em localizações fora dela. A solicitação deve ser feita pelo gerente do empregado e verificada conforme descreve a seção Procedimentos de Verificação e Autorização.

Explicação/Observações: O reconhecimento da necessidade do acesso à rede corporativa fora dela por pessoal autorizado e a limitação de tal acesso apenas ao pessoal que precisa dele pode diminuir bastante o risco e o gerenciamento dos usuários de acesso remoto. Quanto menor for o número de pessoas que têm privilégios de discagem externa, menor o número de alvos em potencial para um atacante. Nunca se esqueça de que o atacante também pode visar aos usuários remotos com a intenção de seqüestrar sua conexão com a rede corporativa ou mascarando-as durante uma chamada falsa.

7-3 Redefinindo as senhas das contas com privilégios

Política: A solicitação para redefinir uma senha de uma conta com privilégios deve ser aprovada pelo gerente ou administrador do sistema responsável pelo computador no qual está a conta. A nova senha deve ser enviada por meio de mensagem de correio eletrônico interno da empresa ou pessoalmente.

Explicação/Observações: As contas com privilégios têm acesso a todos os recursos e arquivos que estão armazenados no sistema de computadores. Naturalmente, elas merecem a maior proteção possível.

7-4 Acesso remoto do pessoal externo de suporte

Política: Nenhum funcionário externo de suporte (tal como o pessoal do fabricante de hardware ou software) pode ter informações de acesso remoto ou permissão para acessar um sistema de computadores da empresa ou dispositivos relacionados sem uma confirmação da identidade e uma autorização para executar tais serviços. Se o fabricante precisar de acesso privilegiado para fornecer serviços de suporte, a senha da conta usada por ele deve ser imediatamente alterada após os serviços estarem concluídos.

Explicação/Observações: Os atacantes podem se fazer passar por fornecedores para terem acesso à rede de computadores ou de telecomunicações da empresa. Assim sendo, é essencial que a

identidade do fornecedor seja verificada, além de sua autorização para executar qualquer trabalho que seja feito no sistema. Além disso, as portas do sistema devem ser fechadas após o seu trabalho ser realizado. Isso é feito alterando-se a senha de conta usada pelo fornecedor.

Nenhum fornecedor deve poder escolher sua própria senha para uma conta, mesmo que seja temporariamente. Alguns fabricantes usam uma senha igual ou semelhante nos sistemas de todos os clientes. Por exemplo, uma empresa de serviços de rede configura as contas privilegiadas em todos os sistemas de seus clientes com a mesma senha e, para aumentar o dano, com o acesso externo via Telnet.

7-5 Autenticação segura para o acesso remoto aos sistemas corporativos

Política: Todos os pontos de conexão da rede corporativa de localizações remotas devem estar protegidos com o uso dos dispositivos de autenticação segura, tais como as senhas dinâmicas *(tecnologias one-time password)* ou a biométrica.

Explicação/Observações: Muitas empresas dependem das senhas estáticas como o único meio de autenticação dos usuários remotos. Essa prática e perigosa porque ela é insegura: os intrusos dos computadores visam qualquer ponto de acesso remoto que possa ser o elo fraco na rede da vítima. Lembre-se de que você nunca sabe quando outra pessoa conhece a sua senha.

Da mesma forma, todos os pontos de acesso remotos devem estar protegidos com autenticação segura, tal como tokens baseados em tempo, cartões inteligentes ou dispositivos de biométrica, para que as senhas interceptadas não tenham nenhum valor para um atacante.

Quando a autenticação baseada nas senhas dinâmicas não é prática, os usuários de computadores devem seguir religiosamente a política para escolher senhas difíceis de serem adivinhadas.

7-6 Configuração do sistema operacional

Política: Os administradores de sistema devem sempre que possível garantir que os sistemas operacionais estejam configurados para serem consistentes com todas as políticas e os procedimentos de segurança adequados.

Explicação/Observações: A criação e distribuição das políticas de segurança é uma etapa fundamental na direção da redução do risco, mas, na maioria dos casos, o cumprimento das políticas é deixado para cada empregado. Existem, porém, algumas políticas relacionadas com computadores que podem ser obrigatórias por meio das definições do sistema operacional, tais como o tamanho exigido para as senhas. A automação das políticas de segurança pela configuração dos parâmetros do sistema operacional tira efetivamente a decisão das mãos do elemento humano e aumenta a segurança geral da organização.

7-7 Vencimento obrigatório

Política: Todas as contas de computadores devem ser definidas para expirar após um ano.

Explicação/Observações: A intenção desta política é eliminar a existência das contas de computadores que não estão mais sendo usadas, uma vez que os invasores em geral visam as contas inativas. O processo garante o desativamento automático de todas as contas de computadores que foram mantidas inadvertidamente e que pertencem a ex-empregados ou ex-contratados.

A critério da gerência, você pode exigir que os empregados façam um curso de atualização em segurança na hora da renovação ou que examinem as políticas de segurança das informações e assinem um documento dizendo que concordam em segui-las.

7-8 Endereços de correio eletrônico genéricos

Política: O departamento de tecnologia da informação deve configurar um endereço de correio eletrônico genérico para cada departamento da organização que se comunica com o público.

Explicação/Observações: O endereço de correio eletrônico genérico pode ser divulgado para o público pela recepcionista ao telefone ou pode ser publicado no site Web da empresa. Caso contrário, cada empregado só deve divulgar o seu endereço de correio eletrônico pessoal para quem tenha uma necessidade real de conhecê-lo.

Durante a primeira fase de um ataque da engenharia social, o atacante quase sempre tenta obter os números de telefone, os nomes e os cargos dos empregados. Na maioria dos casos, essas informações estão disponíveis no site Web da empresa ou é só pedi-las. A criação de caixas de correio de voz e/ou endereços de correio eletrônico genéricos dificulta a associação dos nomes dos empregados a determinados departamentos ou responsabilidades.

7-9 Informações de contato para registros de domínio

Política: Ao serem registradas para obtenção de endereço na Internet ou nomes de hosts, as informações de contato do pessoal administrativo, técnico ou outros não devem identificar nenhum funcionário pelo nome. Em vez disso, você deve relacionar um endereço de correio eletrônico genérico e o número de telefone principal da empresa.

Explicação/Observações: A finalidade desta política é evitar que as informações de contato sejam usadas por um intruso. Quando os nomes e os números de telefone dos indivíduos são fornecidos, um intruso pode usar essas informações para entrar em contato com eles e tentar fazer com que revelem as informações do sistema ou executem uma ação que facilite o objetivo do atacante. O engenheiro social também pode se fazer passar por uma pessoa relacionada para tentar enganar os outros funcionários da empresa.

Em vez de um endereço de correio eletrônico de determinado empregado, as informações de contato devem ter a forma de administrador@empresa.com. O pessoal do departamento de telecomunicações pode estabelecer uma caixa de correio por voz genérica para os contatos administrativos ou técnicos, de modo a limitar a divulgação das informações que poderiam ser úteis em um ataque da engenharia social.

7-10 Instalação das atualizações de segurança e do sistema operacional

Política: Todas as correções de segurança do sistema operacional e dos aplicativos devem ser instaladas assim que se tornarem disponíveis. Se esta política entrar em conflito com a operação dos sistemas de produção de missão crítica, tais atualizações devem ser executadas assim que possível.

Explicação/Observações: Quando uma vulnerabilidade é identificada, o fabricante do software deve ser imediatamente contatado para determinar se há um patch ou uma correção temporária para resolver a vulnerabilidade. Um sistema de computador sem patches representa uma das maiores

ameaças à segurança da empresa. Quando os administradores de sistema adiam a aplicação das correções necessárias, a janela de exposição fica muita aberta e qualquer atacante pode invadi-la.

Dezenas de vulnerabilidades de segurança são identificadas e publicadas todas as semanas na Internet. Mesmo que a equipe de tecnologia da informação esteja vigilante em seus esforços de aplicar todas as correções de segurança assim que possível, e apesar de esses sistemas estarem atrás do firewall da empresa, a rede corporativa sempre estará correndo o risco de sofrer um incidente de segurança. E importante conhecer as vulnerabilidades de segurança publicadas e identificadas no sistema operacional ou em qualquer programa de aplicativo usado durante a realização dos negócios.

7-11 Informações de contato nos sites Web

Política: O site Web externo da empresa não deve revelar nenhum detalhe da estrutura corporativa, nem deve identificar os empregados pelo nome.

Explicação/Observações: As informações da estrutura corporativa, tais como os gráficos organizacionais, os quadros de hierarquia, as listas de empregados ou departamentos, a estrutura hierárquica, os nomes, as posições, os números internos para contato, os números dos empregados ou informações semelhantes que sejam usadas para processos internos não devem ser disponibilizados em sites Web que podem ser acessados pelo público.

Os intrusos de computadores quase sempre obtêm informações muito úteis no site Web de um alvo. Eles usam essas informações para se parecer com um empregado com conhecimentos ao usar um pretexto ou um truque. O engenheiro social tem mais chances de estabelecer credibilidade com essas informações à sua disposição. Além disso, ele pode analisar essas informações para descobrir os prováveis alvos que têm acesso a informações valiosas, confidenciais ou críticas.

7-12 Criação de contas com privilégios

Política: Nenhuma conta com privilégio deve ser criada e nenhum sistema de privilégios deve ser concedido a todas as contas, a menos que isso seja autorizado pelo administrador ou gerente do sistema.

Explicação/Observações: Os intrusos de computadores com freqüência fazem-se passar por fornecedores de hardware ou software e tentam fazer com que o pessoal de tecnologia de informações crie contas não autorizadas. A intenção desta política é bloquear esses ataques, estabelecendo maior controle sobre a criação das contas privilegiadas. O gerente ou administrador do sistema de computadores deve aprovar todas as solicitações de criação de uma conta com privilégios elevados.

7-1 3 Contas de convidados

Política: As contas de convidados de todos os sistemas de computadores ou sistemas de dispositivos em rede relacionados devem ser desativadas ou removidas, exceto para um servidor de FTP (file transfer protocol) aprovado pela gerência com o acesso anônimo ativado.

Explicação/Observações: A intenção da conta de convidado é fornecer o acesso temporário às pessoas que não precisam ter sua própria conta. Vários sistemas operacionais estão instalados como default com uma conta de convidado ativada. Essas contas sempre devem ser desativadas por-

que a sua existência viola o princípio da responsabilidade do usuário. A TI deve poder fazer a auditoria de toda a atividade relacionada com computadores e relacioná-la com um usuário específico.

Os engenheiros sociais podem aproveitar essas contas de convidados para ter acesso não autorizado, seja diretamente, seja enganando o pessoal autorizado para usar uma conta de convidado.

7-14 Criptografia dos dados de backup fora da empresa

Política: Todos os dados da empresa que estão armazenados fora dela devem ser criptografados para evitar o acesso não autorizado.

Explicação/Observações: A equipe de operações deve garantir que todos os dados possam ser recuperados no caso de as informações precisarem ser restauradas. Isso exige testes regulares de decriptografia de uma amostragem aleatória de arquivos criptografados para ter certeza de que os dados podem ser recuperados. Além disso, as chaves usadas para criptografar os dados devem ser entregues a um gerente de confiança para o caso de se perderem ou serem inutilizadas.

7-1 5 Acesso de visitante às conexões de rede

Política: Todos os pontos de acesso Ethernet públicos devem estar em uma rede segmentada para evitar o acesso não autorizado à rede interna.

Explicação/Observações: A intenção desta política é evitar que as pessoas de fora se conectem à rede interna quando estiverem nas instalações da empresa. Os conectores Ethernet instalados nas salas de reuniões, no refeitório, nos centros de treinamento ou em outras áreas que podem ser acessadas pelos visitantes devem ser filtrados para evitar o acesso não autorizado de visitantes aos sistemas corporativos de computadores.

A rede ou o administrador de segurança podem optar por configurar uma LAN virtual em um comutador, se houver um, para controlar o acesso àquelas localizações.

7-16 Modems de discagem

Política: Os modems usados para as ligações de discagem devem ser definidos para responder só depois do quarto toque.

Explicação/Observações: Como é descrito no filme *Jogos de Guerra,* os hackers usam uma técnica conhecida como discagem de guerra para localizar as linhas telefônicas que tenham modems conectados a elas. O processo começa com o atacante identificando os prefixos telefônicos usados na área na qual a empresa-alvo está localizada. Um programa de rastreamento é usado para tentar cada número de telefone com aqueles prefixos e localizar aquele que responde com um modem. Para agilizar o processo, esses programas são configurados para aguardar um ou dois toques até receber uma resposta de modem antes de tentar o próximo número. Quando uma empresa define a resposta automática nas linhas de modem com pelo menos quatro toques, os programas de rastreamento não reconhecem a linha como uma linha de modem.

7-1 7 Software antivírus

Política: Cada sistema de computador deve ter versões atualizadas do software antivírus instaladas e ativadas,

Explicação/Observações: Nas empresas que não descarregam automaticamente o software antivírus e os arquivos de definições (os programas que reconhecem os padrões comuns ao software de vírus para reconhecer os vírus novos) nos desktops ou nas estações de trabalho do usuário, cada usuário deve assumir a responsabilidade da instalação e manutenção do software em seus próprios sistemas, incluindo todos os sistemas de computadores usados para acessar remotamente a rede corporativa.

Se for viável, esse software deve ser definido para a atualização automática e noturna das assinaturas de vírus. Quando os arquivos de definições ou assinatura não são descarregados para os desktops dos usuários, estes devem ter a responsabilidade de atualizar os arquivos de definições pelo menos uma vez por semana.

Essas medidas aplicam-se a todas as máquinas desktop e laptops usados para acessar os sistemas de computadores da empresa, e devem ser seguidas mesmo que o computador seja de propriedade da empresa ou pessoal.

7-1 8 Anexos de mensagens de correio eletrônico recebidas (requisitos de alta segurança)

Política: Em uma organização com requisitos altos de segurança, o firewall corporativo deve ser configurado para filtrar todos os anexos de correio eletrônico.

Explicação/Observações: Esta política aplica-se apenas às empresas que têm requisitos de segurança altos ou àquelas que não têm uma necessidade comercial de receber anexos por meio de mensagens de correio eletrônico.

7-19 Autenticação de software

Política: Todo software, correção ou atualização de software novo, seja em mídia física ou obtida pela Internet, deve ter sua autenticidade verificada antes da instalação. Esta política é particularmente relevante para o departamento de TI quando for instalado qualquer software que requer privilégios de sistema.

Explicação/Observações: O software de computador referido nesta política inclui os componentes do sistema operacional, o software de aplicativo, as correções emergenciais, os patches ou quaisquer atualizações de software. Muitos fabricantes de software implementaram métodos pelos quais os clientes podem verificar a integridade de uma distribuição, em geral por meio de uma assinatura digital. Em qualquer caso no qual a integridade não possa ser verificada, o fabricante deve ser consultado para confirmar se o software é autêntico.

Os atacantes de computadores enviam para uma vítima um software embalado como se o fabricante o tivesse produzido e enviado para a empresa. E essencial que você verifique a autenticidade de todo software recebido, particularmente se ele não foi pedido, antes de instalá-lo nos sistemas da empresa.

Saiba que um atacante sofisticado pode descobrir que a sua organização encomendou o software de um fabricante. Com essa informação em mãos, ele pode cancelar o pedido com o fabricante real e pedir o software ele mesmo. Em seguida, o software é modificado para executar alguma função maliciosa e é enviado ou entregue em sua empresa, no pacote original, com a embalagem adequada. se for preciso. Após a instalação do produto, o atacante tem o controle.

7-20 Senha-padrão

Política: Todo software de sistema operacional e dispositivo de hardware que tenha uma senha definida com um valor-padrão deve ser redefinido de acordo com a política de senhas da empresa.

Explicação/Observações: Vários sistemas operacionais e dispositivos de computador relacionados são enviados com senhas-padrão — ou seja, com a mesma senha ativa em cada unidade que é vendida. Um grave erro é não alterar as senhas-padrão, porque isso significa um risco para a empresa.

As senhas-padrão são conhecidas de todos e estão disponíveis nos sites Web na Internet. Em um ataque, a primeira senha que um intruso tenta é a senha-padrão do fabricante.

7-21 Bloqueio por tentativas inválidas de acesso (segurança baixa a média)

Política: Em uma organização com requisitos de segurança de nível baixo a médio, sempre que um número especificado de tentativas sucessivas e inválidas de login em determinada conta for feito, a conta deve ser bloqueada por um período de tempo.

Explicação/Observações: Todas as estações de trabalho e servidores da empresa devem ser definidos para limitar o número de tentativas sucessivas e inválidas de login. Esta política e necessária para evitar a adivinhação de senha pela tentativa e erro, pelos ataques aos dicionários ou pelas tentativas de força bruta para ter acesso não autorizado.

O administrador de sistema deve configurar as definições de segurança para bloquear uma conta sempre que o limite desejado de tentativas sucessivas e inválidas for atingido. Recomendamos que uma conta seja bloqueada por pelo menos 30 minutos após sete tentativas sucessivas e inválidas de login.

7-22 Bloqueio por tentativas inválidas de acesso (alta segurança)

Política: Em uma organização com altos requisitos de segurança, sempre que um número especificado de tentativas inválidas e sucessivas de login em determinada conta for feito, a conta deve ser desativada até que seja redefinida pela pessoa do grupo responsável por fornecer suporte de conta.

Explicação/Observações: Todas as estações de trabalho e servidores da empresa devem ser definidos para limitar o número de tentativas sucessivas e inválidas de login. Esta política é um controle necessário para evitar que uma senha seja adivinhada pela tentativa e erro. pelos ataques de dicionário ou pelas tentativas de força bruta de ter acesso não autorizado.

O administrador do sistema deve configurar as definições de segurança para bloquear uma conta após cinco tentativas inválidas de login. Depois de tal ataque, o dono da conta terá de ligar para o suporte técnico ou para a pessoa do grupo responsável pelo suporte de conta para ativá-la. Antes de redefinir a conta, o responsável pelo departamento deve confirmar a identidade do dono da conta, de acordo com os Procedimentos de Verificação e Autorização.

7-23 Alteração periódica das senhas de conta com privilégios administrativos

Política: Todos os donos de contas com privilégios administrativos devem alterar suas senhas pelo menos a cada 30 dias.

Explicação/Observações: Dependendo das limitações do sistema operacional, o administrador de sistemas deve implantar essa política pela configuração dos parâmetros de segurança no software de sistema.

7-24 Alteração periódica das senhas de usuário

Política: Todos os donos de contas devem alterar suas senhas pelo menos a cada 60 dias.

Explicação/Observações: Nos sistemas operacionais que fornecem este recurso, o administrador de sistemas deve implantar esta política pela configuração dos parâmetros de segurança no software.

7-25 Configuração de senha de conta nova

Política: As contas novas de computador devem ser estabelecidas com uma senha inicial com vencimento prévio, para que o dono da conta tenha de selecionar uma senha nova ao iniciar o uso.

Explicação/Observações: Este requisito garante que apenas o dono da conta tenha conhecimento de sua senha.

7-26 Senhas de inicialização

Política: Todos os sistemas de computador devem estar configurados para exigir uma senha de inicialização.

Explicação/Observações: Os computadores devem estar configurados para solicitar uma senha ao serem ligados e antes de o sistema operacional ser inicializado. Isso evita que uma pessoa não autorizada ligue e use o computador de outra pessoa. Esta política aplica-se a todos os computadores das instalações da empresa.

7-27 Requisitos de senha para as contas privilegiadas

Política: Todas as contas com privilégios devem ter uma senha segura com estas características:

- Ela não pode ser uma palavra encontrada em um dicionário de qualquer idioma.
- Ela deve combinar pelo menos uma letra maiúscula ou minúscula, um símbolo e um numeral.
- Ela deve ter pelo menos 12 caracteres de comprimento.
- Ela não pode estar relacionada à empresa ou ao indivíduo.

Explicação/Observações: Na maioria dos casos os invasores visam as contas específicas que tenham privilégios de sistema. Eventualmente, o atacante explora outras vulnerabilidades para ter controle completo sobre o sistema.

As primeiras senhas que um intruso tenta são as palavras simples, mais usadas e encontradas em um dicionário. A seleção de senhas seguras melhora a segurança, reduzindo as chances de que um atacante a encontre por tentativa e erro, ataque a dicionário ou ataque de força bruta.

7-28 Pontos de acesso sem fio

Política: Todos os usuários que podem acessar uma rede sem fio devem usar a tecnologia VPN (Virtual Private Network) para proteger a rede corporativa.

Explicação/Observações: As redes sem fio estão sendo atacadas por uma nova técnica chamada *direção de guerra.* Nessa técnica o invasor simplesmente dirige ou caminha com um laptop equipado com uma placa 802.11B NIC até que uma rede sem fio seja detectada.

Muitas empresas empregam as redes sem fio sem ativar o WEP (wireless equivalency protocol), o qual é usado para dar segurança à conexão sem fio por meio do uso da criptografia. Mas mesmo quando está ativada, a versão atual do WEP (lançada na metade de 2002) não é efetiva: ela ficou aberta e vários sites Web dedicam-se a fornecer o meio de localizar os sistemas sem fio abertos e entrar nos pontos de acesso sem fio ativados para o WEP.

Da mesma forma, é essencial incluir uma camada de proteção ao redor do protocolo 802.11B empregando a tecnologia VPN.

7-29 Atualizando os arquivos de definições do antivírus

Política: Cada sistema de computador deve estar programado para atualizar automaticamente os arquivos de definição antivírus e contra o Cavalo de Tróia.

Explicação/Observações: No mínimo, tais atualizações devem ocorrer pelo menos semanalmente. Nas empresas nas quais os empregados deixam seus computadores ligados, esses arquivos de definições devem ser atualizados todas as noites. O software antivírus não é efetivo porque ele não é atualizado para detectar todas as novas formas de código malicioso. Como a ameaça de infecções por vírus, worm e Cavalo de Tróia aumenta substancialmente quando os arquivos de definições não são atualizados, é essencial que os produtos antivírus ou anticódigo malicioso sejam mantidos atualizados.

Operações de computadores

8-1 Inserindo comandos ou executando programas

Política: O pessoal que opera o computador não deve inserir comandos ou executar programas sob solicitação de qualquer pessoa que ele não conheça. Se surgir uma situação na qual uma Pessoa Não Verificada parecer ter um motivo para fazer tal solicitação, ela não deve ser atendida sem antes haver aprovação do gerente.

Explicação/Observações: Os funcionários que operam com computador são alvos conhecidos dos engenheiros sociais, uma vez que as suas posições em geral exigem acesso de conta com privilégios e o atacante espera que eles tenham menos experiência e menos conhecimento sobre os procedimentos da empresa do que os outros funcionários de TI. A intenção desta política é incluir uma verificação apropriada para evitar que os engenheiros sociais enganem o pessoal que opera os computadores.

8-2 Funcionários com contas com privilégios

Política: Os funcionários que têm contas com privilégios não devem fornecer assistência ou informações para nenhuma Pessoa Não Verificada. Em particular esta política dita que não se deve fornecer ajuda com o computador (tal como treinamento sobre o uso de aplicativos), acesso a algum banco de dados da empresa, download de software nem revelar nomes de pessoas que tenham capacidade de acesso remoto.

Explicação/Observações: Os engenheiros sociais quase sempre visam os empregados que têm contas com privilégios. A intenção desta política é orientar a equipe de TI que tem contas com privilégios para que ela saiba lidar com as ligações que podem representar ataques da engenharia social.

8-3 Informações dos sistemas internos

Política: A equipe de Operações de Computador nunca deve divulgar nenhuma informação relacionada com os sistemas de computadores da empresa ou dispositivos relacionados sem confirmar a identidade do solicitante.

Explicação/Observações: Os invasores de computadores quase sempre entram em contato com os empregados de operações para obter informações valiosas, tais como os procedimentos de acesso ao sistema, os pontos externos de acesso remoto e os números de telefone de discagem que têm valor substancial para eles.

Nas empresas que têm equipe de suporte técnico ou um help desk, as solicitações feitas para a equipe de operações de computador pedindo informações sobre sistemas de computadores ou dispositivos relacionados devem ser consideradas incomuns. Toda solicitação de informação deve ser examinada de acordo com a política de classificação de dados corporativa para determinar se o solicitante está autorizado a ter tais informações. Quando a classe das informações não puder ser determinada, elas devem ser consideradas como Internas.

Em alguns casos, o suporte técnico do fornecedor externo terá de se comunicar com as pessoas que têm acesso aos sistemas de computadores da empresa. Eles devem ter contatos específicos no departamento de TI para que os envolvidos possam reconhecer uns aos outros para fins de verificação.

8-4 Divulgação de senhas

Política: A equipe de operações de computador nunca deve revelar suas senhas ou nenhuma outra senha que lhe seja confiada sem aprovação prévia de um gerente de tecnologia da informação.

Explicação/Observações: Em lermos gerais, a revelação de qualquer senha para outra pessoa é proibida. Esta política reconhece que o pessoal de operações talvez tenha de revelar uma senha para terceiros quando surgem situações urgentes. Esta exceção à política geral que proíbe a divulgação de qualquer senha requer aprovação específica de um gerente de tecnologia da informação. Como medida extra de precaução, esta responsabilidade de divulgar informações de autenticação deve se limitar a um grupo pequeno de indivíduos que receberam treinamento especial sobre os procedimentos de verificação.

8-5 Mídia eletrônica

Política: Toda mídia eletrônica que contenha informações que não foram criadas para liberação ao público deve ser mantida em uma localização fisicamente segura.

Explicação/Observações: A intenção desta política é evitar o roubo físico de informações Sigilosas armazenadas em mídia eletrônica.

8-6 Mídia de backup

Política: O pessoal de operações deve armazenar a mídia de backup em um cofre da empresa ou em outra localização segura.

Explicação/Observações: A mídia de backup é outro alvo primário dos invasores de computadores. Um atacante não vai perder tempo tentando comprometer um sistema ou rede de computadores quando o elo mais fraco da cadeia pode ser a mídia de backup fisicamente desprotegida. Após a mídia de backup ser roubada, o atacante pode comprometer a confidencialidade dos dados armazenados nela, a menos que estejam criptografados. Assim sendo, dar segurança física à mídia de backup e um processo essencial para proteger a confidencialidade das informações corporativas.

POLÍTICAS PARA TODOS OS EMPREGADOS

Tanto no departamento de TI, de recursos humanos, no departamento contábil ou na equipe de manutenção existem determinadas políticas de segurança que cada empregado da sua empresa deve conhecer. Essas políticas classificam-se nas categorias, Geral, Uso do Computador, Uso do Correio Eletrônico, políticas para Telecomutadores, Uso do Telefone, Uso do Fax, Uso do Voice Mail e Senhas,

Geral

9-1 Relatando ligações suspeitas

Política: Os empregados que suspeitam que podem estar sendo alvos de uma violação de segurança, incluindo todas as solicitações suspeitas de divulgação de informações ou de execução de ações em um computador, devem relatar o evento imediatamente ao grupo de relatório de incidentes da empresa.

Explicação/Observações: Quando um engenheiro social não convence o seu alvo a atender uma exigência, ele sempre tenta outra pessoa. Ao relatar uma ligação ou um evento suspeito, um empregado toma a primeira etapa para alertar a empresa de que um ataque pode estar a caminho. Assim sendo. os empregados individuais são a linha de frente na defesa contra os ataques da engenharia social.

9-2 Documentando as ligações suspeitas

Política: No caso de uma ligação telefônica suspeita que parece ser um ataque de engenharia social, o empregado deve, na medida do possível, conversar com o interlocutor para saber dos detalhes que possam revelar o que o atacante está tentando conseguir e tomar notas desses detalhes para depois fazer um relatório.

Explicação/Observações: Quando reportados ao grupo de relatório de incidentes, tais detalhes podem ajudá-los a detectar o objeto ou padrão de um ataque.

9-3 Divulgação dos números de discagem

Política: Os funcionários da empresa não devem divulgar os números de telefone de modem da empresa, mas sempre devem encaminhar tais solicitações para o help desk ou pessoal do suporte técnico.

Explicação/Observações: Os números de telefone de discagem devem ser tratados como informações Internas e só devem ser fornecidos a empregados que tenham necessidade de ter essas informações para executar seu trabalho.

Os engenheiros sociais geralmente visam os empregados ou departamentos que podem proteger menos as informações solicitadas. Por exemplo, o atacante pode ligar para o departamento de contas a pagar fazendo-se passar por um empregado da empresa de telefonia que está tentando resolver um problema com uma fatura. Em seguida, pede alguns números de fax ou discagem conhecidos para resolver o problema. O intruso quase sempre visa um empregado que não tem chances de perceber o perigo de liberar tais informações ou que não tem o treinamento com relação à política e aos procedimentos de divulgação da empresa.

9-4 Crachás de identificação da empresa

Política: Exceto quando estiver na área próxima ao escritório, todo funcionário da empresa, incluindo a gerencia e a equipe executiva, deve usar seus crachás de empregado durante todo o tempo.

Explicação/Observações: Todos os funcionários, incluindo os executivos corporativos, devem ser treinados e motivados para entender que o uso de um crachá de identificação é obrigatório em qualquer lugar das instalações da empresa que não sejam áreas públicas e o próprio escritório ou grupo de trabalho da pessoa.

9-5 Desafiando os que não usam crachá de identificação

Política: Todos os empregados devem questionar imediatamente qualquer pessoa desconhecida que não esteja usando um crachá de empregado ou visitante.

Explicação/Observações: Embora nenhuma empresa queira criar uma cultura na qual os empregados fiquem procurando um modo de questionar os colegas que se aventuram a ir até o saguão sem seus crachás, toda empresa que se preocupa em proteger suas informações precisa levar a sério a ameaça de um engenheiro social perambulando pelas suas instalações sem ser questionado. A motivação para que os empregados sejam diligentes e ajudem a implantar a política de sempre usar o crachá inclui, por exemplo, o reconhecimento da iniciativa no jornal da empresa ou nos quadros de avisos; algumas horas de licença remunerada ou uma carta de recomendação em seus registros pessoais.

9-6 Burlando a segurança da entrada

Política: Os empregados que entram em um prédio não devem permitir que ninguém que eles não conheçam pessoalmente os siga quando usarem um meio seguro, tal como um cartão-chave, para entrar no prédio.

Explicação/Observações: Os empregados devem entender que não é falta de educação exigir que as pessoas desconhecidas se identifiquem antes de ajudá-las a entrar em um prédio ou acessar uma área segura.

Com freqüência, os engenheiros sociais usam uma técnica conhecida como "pular sela", porque ficam ao lado de outra pessoa que está entrando em um prédio ou área Sigilosa e, em seguida, simplesmente entram com essa pessoa. A maioria das pessoas não se sente bem em questionar as outras pessoas, supondo que talvez sejam empregados legítimos. Outra técnica semelhante é transportar diversas caixas para que o trabalhador abra e mantenha a porta aberta para ajudar.

9-7 Destruindo documentos sigilosos

Política: Os documentos sigilosos a ser descartados devem ser colocados em uma máquina de cortar papel; a mídia, incluindo discos rígidos que alguma vez contiveram informações ou materiais Sigilosos, deve ser destruída de acordo com os procedimentos estabelecidos pelo grupo responsável pela segurança das informações.

Explicação/Observações: As máquinas-padrão de cortar papel não destroem adequadamente os documentos. As máquinas com corte cruzado transformam os documentos em polpa. A melhor prática de segurança é presumir que os principais concorrentes da organização revirarão os materiais descartados em busca de qualquer informação que possa beneficiá-los.

Os espiões industriais e atacantes de computador obtêm regularmente as informações Sigilosas dos materiais que são jogados no lixo. Em alguns casos, os concorrentes têm tentado enganar as equipes de limpeza para mexer no lixo da empresa. Em um exemplo recente, um empregado da Goldman Sachs descobriu na lata de lixo itens que foram usados em um esquema interno de comércio.

9-8 Identificadores pessoais

Política: Os identificadores pessoais, tais como o número do empregado, o número do seguro social, o número da carteira de motorista, a data e o local de nascimento e o nome de solteira da mãe nunca devem ser usados como um meio de verificar a identidade. Esses identificadores não são secretos e podem ser obtidos por inúmeros meios.

Explicação/Observações: Um engenheiro social pode obter os identificadores pessoais de outras pessoas por um preço. E, na verdade, ao contrário da crença popular, todos que têm um cartão de crédito e acesso à Internet podem obter essas identificações pessoais. Mesmo assim, apesar do perigo óbvio, os bancos, as empresas de serviços públicos e as administradoras de cartões de crédito normalmente usam esses identificadores. Esse é um dos motivos pelos quais o roubo de identidade é o crime de crescimento mais rápido da década.

9-9 Organogramas

Política: Os detalhes mostrados no organograma não devem ser divulgados para ninguém além dos empregados da empresa.

Explicação/Observações: As informações sobre a estrutura corporativa incluem os organogramas, as listas departamentais de empregados, os nomes dos empregados, as posições dos empregados, os números de contato internos, os números de empregados ou informações semelhantes.

Na primeira fase de um ataque da engenharia social, o objetivo é reunir informações sobre a estrutura interna da empresa. Em seguida, essas informações são usadas para criar um plano de

ataque. O atacante também pode analisar essas informações para determinar quais empregados podem ter acesso aos dados que ele busca. Durante o ataque, as informações fazem o atacante parecer um empregado bem informado, e isso lhe dá mais chances de fazer com que a vítima coopere.

9-10 Informações particulares sobre os empregados

Política: Todas as solicitações de informações particulares sobre um empregado devem ser encaminhadas para o departamento de recursos humanos.

Explicação/Observações: Uma exceção a esta política pode ser o número de telefone para um empregado que precisa ser contatado por motivos profissionais ou que esteja agindo como intermediário. Entretanto, sempre é preferível obter o número de telefone do solicitante e fazer com que o empregado ligue de volta para a pessoa.

Uso do computador

10-1 Inserindo comandos em um computador

Política: Os funcionários nunca devem inserir comandos em um computador ou equipamento relacionado sob solicitação de outra pessoa, a menos que o solicitante tenha sido verificado como um empregado do departamento de tecnologia da informação.

Explicação/Observações: Um truque comum dos engenheiros sociais é solicitar que um empregado insira um comando que faz uma alteração na configuração do sistema e permita que o atacante acesse o computador da vitima sem fornecer autenticação ou recupere as informações que podem ser usadas para facilitar um ataque técnico.

10-2 Convenções internas de nomeação

Política: Os funcionários não devem divulgar os nomes internos dos sistemas ou bancos de dados de computadores sem verificação prévia de que o solicitante é empregado da empresa.

Explicação/Observações: Às vezes os engenheiros sociais tentam obter os nomes dos sistemas de computadores da empresa. Depois de ter um nome, o atacante faz uma ligação para a empresa fazendo-se passar por um empregado legítimo que está com problemas para acessar ou usar um dos sistemas. Conhecendo o nome interno designado a determinado sistema, o engenheiro social adquire credibilidade.

10-3 Solicitações para executar programas

Política: Os funcionários nunca devem executar nenhum aplicativo ou programa de computador sob solicitação de outra pessoa, a menos que o solicitante tenha sido verificado como um empregado do departamento de tecnologia da informação.

Explicação/Observações: Toda solicitação para executar programas, aplicativos ou executar qualquer atividade em um computador deve ser recusada, a menos que o solicitante seja identificado positivamente como um empregado do departamento de tecnologia da informação. Se a solicitação envolver a revelação de informações Confidenciais de qualquer arquivo ou mensagem

eletrônica, a resposta ao solicitante deve estar de acordo com os procedimentos para liberação das informações Confidenciais. Consulte a Política de Divulgação de Informações.

Os atacantes enganam as pessoas para que elas executem programas que permitam ao intruso ter o controle do sistema. Quando um usuário desavisado executa um programa "plantado" por um atacante, o resultado pode dar ao intruso o acesso ao sistema de computadores da vítima. Outros programas registram as atividades do usuário do computador e retornam essas informações para o atacante.

Enquanto um engenheiro social pode enganar uma pessoa para que ela execute instruções no computador que podem causar danos, um ataque técnico engana o sistema operacional para executar instruções de computador que podem causar o mesmo tipo de danos.

10-4 Fazendo download ou instalando software

Política: Os funcionários nunca devem fazer download ou instalar software sob solicitação de outra pessoa, a menos que o solicitante tenha sido verificado como um empregado do departamento de tecnologia da informação.

Explicação/Observações: Os empregados devem estar alertas para qualquer solicitação incomum que envolva qualquer tipo de transação com equipamento relacionado com computadores.

Uma tática comum usada pelos engenheiros sociais e enganar as vitimas desavisadas para que façam o download e instalem um programa que ajude o atacante a realizar o seu objetivo de comprometer a segurança do computador ou da rede. Em alguns casos, o programa pode espiar e registrar as ações do usuário ou permitir que o atacante assuma o controle do sistema de computadores usando um aplicativo remoto por meio de conexões criptografadas.

10-5 Senhas em texto simples e correio eletrônico

Política: As senhas não devem ser enviadas por correio eletrônico, a menos que sejam criptografadas.

Explicação/Observações: Embora não seja desencorajada, esta política não é usada pelos sites de comércio eletrônico em determinadas circunstâncias, tais como:

- O envio de senhas para clientes que se registraram no site.
- O envio de senhas para os clientes que perderam ou se esqueceram de suas senhas.

10-6 Software relacionado à segurança

Política: Os funcionários nunca devem remover ou desativar antivírus, firewall ou outro software relacionado com segurança sem a prévia aprovação do departamento de tecnologia da informação.

Explicação/Observações: Os usuários às vezes desativam o software relacionado com segurança ingenuamente, achando que isso vai aumentar a velocidade de seus computadores.

Um engenheiro social pode tentar enganar um empregado para que ele desative ou remova o software que é necessário para proteger a empresa contra as ameaças relacionadas com segurança.

10-7 Instalação de modems

Política: Nenhum modem pode estar conectado a nenhum computador até que a aprovação prévia seja obtida do departamento de TI.

Explicação/Observações: É importante reconhecer que os modems dos desktops ou estações de trabalho representam uma ameaça substancial à segurança, sobretudo se estiverem conectados à rede corporativa. Da mesma forma, esta política controla os procedimentos de conexão por modem.

Os hackers usam uma técnica chamada discagem de guerra para identificar todas as linhas de modem ativas dentro de determinados números de telefone. A mesma técnica pode ser usada para localizar os números de telefone que estão conectados aos modems da empresa. Um atacante pode comprometer facilmente a rede corporativa se identificar um sistema de computadores conectado a um modem que execute software vulnerável de acesso remoto que esteja configurado com uma senha fácil de adivinhar ou nenhuma senha.

10-8 Modems e definições de resposta automática

Política: Todos os desktops ou estações de trabalho com modems aprovados pelo TI devem ter o recurso de resposta automática desativado para evitar que alguém disque para o sistema de computadores.

Explicação/Observações: Sempre que possível, o departamento de tecnologia da informação deve empregar um conjunto de modems de discagem para aqueles funcionários que precisam discar para sistemas de computadores externos via modem.

10-9 Ferramentas de invasão

Política: Os empregados não devem fazer o download nem usar ferramentas de software criadas para anular os mecanismos de proteção de software.

Explicação/Observações: A Internet tem dezenas de sites que armazenam softwares criados para quebrar chaves de segurança de ferramentas shareware e comerciais. O uso desses programas não apenas viola o copyright do proprietário de um software, mas também é muito perigoso. Como esses programas originam-se de fontes desconhecidas, eles podem conter códigos ocultos de caráter malicioso que pode causar danos ao computador do usuário ou plantar um Cavalo de Tróia que dá ao invasor acesso total ao computador do usuário.

10-10 Publicando informações da empresa on-line

Política: Os empregados não devem divulgar nenhum detalhe relativo ao hardware ou software da empresa em newsgroups públicos, fóruns ou bulletin boards e não devem mencionar nenhuma informação de contato interno que não esteja de acordo com a política.

Explicação/Observações: Toda mensagem publicada na Usenet, nos fóruns on-line, nos bulletin boards ou em mailing lists pode ser pesquisada para o atacante reunir as informações sobre a empresa-alvo ou um indivíduo alvo. Durante a fase de pesquisa de um ataque de engenharia social, o atacante pode pesquisar na Internet todas as publicações que contém informações úteis sobre a empresa, seus produtos ou seu pessoal.

Algumas delas contêm informações úteis que o atacante pode usar para melhorar um ataque. Por exemplo, um administrador de rede pode publicar uma pergunta sobre a configuração dos filtros de firewall de determinada marca e modelo. Um atacante que descobre essa mensagem adquire informações valiosas sobre o tipo e a configuração do firewall usado que lhe permite ter acesso à rede da empresa.

Esse problema pode ser reduzido ou evitado pela implementação de uma política que permite que os empregados participem de newsgroups com contas anônimas que não identificam a empresa da qual se originaram. Naturalmente, a política deve exigir que os empregados não incluam nenhuma informação de contato que possa identificar a empresa.

10-11 Disquetes e outra mídia eletrônica

Política: Se uma mídia qualquer, tal como disquetes ou CD-ROMs, for deixada em uma área de trabalho ou na mesa de um empregado, e se aquela mídia for de origem desconhecida, ela não deve ser inserida em nenhum sistema de computadores.

Explicação/Observações: Um método usado pelos atacantes para instalar código malicioso e colocar programas em um disquete ou CD-ROM e rotulá-lo como algo irresistível (por exemplo, "Dados de pagamento do pessoa! - Confidencial"). Em seguida, eles deixam diversas cópias nas áreas usadas pelos empregados. Se uma única cópia for inserida em um computador e os arquivos forem abertos, o código malicioso do atacante será executado. Isso pode criar uma backdoor, que é usada para comprometer o sistema, ou pode causar outros danos para a rede.

10-12 Descartando mídia removível

Política: Antes de descartar qualquer mídia eletrônica que já conteve informações Sigilosas da empresa, mesmo que essas informações já tenham sido excluídas, ela deve ser totalmente destruída ou danificada para que não tenha recuperação.

Explicação/Observações: Embora o uso das máquinas de cortar papel seja comum hoje em dia, os funcionários da empresa podem não dar importância à ameaça de descartar mídia eletrônica que continha dados Sigilosos. Os atacantes tentam recuperar todos os dados armazenados na mídia eletrônica descartada. Os funcionários podem presumir que a simples exclusão dos arquivos garante que esses arquivos não podem ser recuperados. Essa suposição e incorreta e pode fazer com que as informações comerciais confidenciais caiam nas mãos erradas. Da mesma forma, toda mídia eletrônica que contenha ou tenha contido informações que não foram rotuladas como Públicas devem ser limpas ou destruídas usando-se os procedimentos aprovados pelo grupo responsável.

10-13 Protetores de tela com senha

Política: Todos os usuários de computadores devem definir uma senha para a proteção de tela e o limite de inatividade para bloquear o computador após determinado período de inatividade.

Explicação/Observações: Todos os empregados são responsáveis por definir uma senha de proteção de tela e um timeout de inatividade com tempo não superior a dez minutos. A intenção desta política é evitar que uma pessoa não autorizada use o computador de outra pessoa. Além disso, esta política evita que os sistemas de computador da empresa sejam facilmente acessados por estranhos que tenham tido acesso ao prédio.

10-14 Divulgação ou compartilhamento da declaração de senhas

Política: Antes de criar uma nova conta de computador, o empregado ou contratado deve assinar uma declaração por escrito reconhecendo que entende que as senhas nunca devem ser divulgadas ou compartilhadas com qualquer pessoa e que concorda em seguir essa política.

Explicação/Observações: A declaração também deve incluir um aviso de que a violação de tal acordo pode levar a uma ação disciplinar que vai desde uma simples advertência até o desligamento do funcionário.

Uso do correio eletrônico

11-1 Anexos de correio eletrônico

Política: Os anexos de correio eletrônico não devem ser abertos, a menos que seja esperado ou tenha sido enviado por uma Pessoa de Confiança.

Explicação/Observações: Todos os anexos de correio eletrônico devem ser bem examinados. Você pode exigir que uma Pessoa de Confiança dê um aviso prévio de que um anexo está sendo enviado antes de abri-lo. Isso reduzirá o risco de que os atacantes que usam as táticas de engenharia social enganem as pessoas para que elas abram os anexos.

Um método de comprometer um sistema de computador é fazer com que um empregado execute um programa malicioso que cria uma vulnerabilidade e fornece ao atacante o acesso ao sistema. Ao enviar um anexo de correio eletrônico que tem um código executável ou macros, o atacante pode ter o controle do computador do usuário.

Um engenheiro social pode enviar um anexo de correio eletrônico malicioso e, em seguida, pode ligar e tentar persuadir o destinatário para que ele abra o anexo.

11-2 Encaminhamento automático para endereços externos

Política: Deve ser proibido o encaminhamento automático de mensagens recebidas por correio eletrônico para um endereço de correio eletrônico externo.

Explicação/Observações: A intenção desta política é evitar que um estranho receba uma mensagem de correio eletrônico enviada para um endereço de correio eletrônico interno.

Eventualmente os empregados configuram o encaminhamento das mensagens de correio eletrônico recebidas para um endereço fora da empresa quando eles estão fora do escritório. Ou então, um atacante pode conseguir enganar um empregado para que ele configure um endereço de correio eletrônico interno que é encaminhado para um endereço fora da empresa. Em seguida, ele pode se fazer passar como um empregado legítimo que tem um endereço de correio eletrônico interno da empresa e fazer com que as pessoas enviem informações Confidenciais para o endereço de correio eletrônico interno.

11-3 Encaminhando mensagens de correio eletrônico

Política: Toda solicitação de uma Pessoa Não Verificada para transferir uma mensagem de correio eletrônico para outra Pessoa Não Verificada exige a confirmação da identidade do solicitante.

11-4 Verificando as mensagens de correio eletrônico

Política: Uma mensagem de correio eletrônico que pareça ter vindo de uma Pessoa de Confiança e contenha uma solicitação de informações não destinadas ao Público ou um pedido para executar uma ação com qualquer equipamento relacionado com computadores requer um formulário de autenticação adicional. Consulte Procedimentos de Verificação e Autorização.

Explicação/Observações: Um atacante pode forjar facilmente uma mensagem de correio eletrônico e seu cabeçalho para fazer com que ela pareça ter sido originada de outro endereço de correio eletrônico. Ele também pode enviar uma mensagem de correio eletrônico de um sistema de computador comprometido, que forneça uma autorização falsa para divulgar informações ou executar uma ação. Mesmo examinando o cabeçalho de uma mensagem de correio eletrônico. você não pode detectar aquelas que foram enviadas de um sistema interno de computador comprometido.

O uso do telefone

12-1 Participando de pesquisas ao telefone

Política: Os empregados não devem participar de pesquisas nem responder perguntas de qualquer organização ou pessoa estranha. Tais solicitações devem ser encaminhadas para o departamento de relações públicas ou para outra pessoa designada.

Explicação/Observações: Um método usado pelos engenheiros para obter informações valiosas que podem ser usadas contra a empresa é ligar para um empregado e dizer que está fazendo uma pesquisa. E surpreendente o modo como muitas pessoas ficam felizes em fornecer informações sobre a empresa e sobre si mesmos para estranhos quando elas acreditam que estão fazendo parte de uma pesquisa. Entre as questões inofensivas, o atacante insere algumas perguntas que quer saber. Eventualmente, tais informações podem ser usadas para comprometer a rede corporativa.

12-2 Divulgação dos números internos de telefone

Política: Se uma Pessoa Não Verificada pede a um empregado o seu número de telefone, ele primeiro deve determinar se a divulgação do número é necessária para a condução dos negócios da empresa.

Explicação/Observações: A intenção desta política é exigir que os empregados tomem uma decisão bem pensada diante da necessidade ou não da divulgação de seus ramais. Ao lidar com pessoas que não demonstraram uma necessidade genuína de saber o ramal, a decisão mais segura é exigir que liguem para o número de telefone principal da empresa e sejam transferidos.

12-3 Senhas nas mensagens do voice mail

Política: E proibido deixar mensagens que contenham informações de senha na caixa postal do voice mail de alguém.

Explicação/Observações: Um engenheiro social quase sempre pode ter acesso à caixa postal de voz de um empregado porque ela está inadequadamente protegida com um código de acesso fácil de adivinhar. Em um tipo de ataque, um intruso sofisticado pode criar sua própria caixa postal de voz falsa e convencer outro empregado para deixar uma mensagem transmitindo informações de senha. Esta política combate esse golpe.

Uso do fax

1 3-1 Retransmissão de faxes

Política: Nenhum fax deve ser recebido e encaminhado para outra parte sem verificação da identidade do solicitante.

Explicação/Observações: Os ladrões de informações podem enganar os funcionários para que eles enviem informações sigilosas por fax para uma máquina localizada nas instalações da empresa. Antes de o atacante dar o número do fax para a vítima, ele liga para um empregado desavisado, tal como uma secretária ou um assistente administrativo, e pergunta se um documento pode ser enviado para eles por fax para ser retirado mais tarde. Em seguida, após o empregado desavisado ter recebido o fax, o atacante liga para ele e solicita que o fax seja enviado para outra localização, alegando talvez que ele é necessário para uma reunião urgente. Como a pessoa que deve retransmitir o fax geralmente não entende o valor das informações, ela atende à solicitação.

1 3-2 Verificação de autorizações por fax

Política: Antes de executar quaisquer instruções recebidas por fax, o remetente deve ser confirmado como um empregado ou Pessoa de Confiança. Geralmente uma ligação telefônica para o remetente para verificar a solicitação é suficiente.

Explicação/Observações: Os empregados devem tomar cuidado quando solicitações incomuns são enviadas por fax, tal como uma solicitação para entrar comandos em um computador ou divulgar informações. Os dados do cabeçalho de um documento enviado por fax podem ser falsificados pela alteração das definições da máquina de fax remetente. Assim sendo, o cabeçalho de um fax não deve ser aceito como um meio de estabelecer a identidade ou autorização.

1 3-3 Enviando informações sigilosas por fax

Política: Antes de enviar informações Sigilosas por fax para uma máquina que esteja localizada em uma área acessada por outros funcionários, o remetente deve transmitir uma página de rosto. O destinatário, ao receber a página, transmite uma página de resposta, para demonstrar que ele está presente fisicamente na máquina de fax. Em seguida, o remetente retransmite o fax.

Explicação/Observações: Este processo garante ao remetente que o destinatário está presente fisicamente no lado receptor. Além disso, confirma se o número do telefone do fax de recepção não foi encaminhado para outra localização.

1 3-4 Proibição de envio de senhas por fax

Política: As senhas não podem ser enviadas por fax sob nenhuma circunstância.

Explicação/Observações: O envio das informações de autenticação por fax não é seguro. A maioria das máquinas de fax pode ser acessada por diversos empregados. Além disso, elas usam a rede pública comutada de telefones, que pode ser manipulada pelo encaminhamento do número de telefone para a máquina de fax receptora, para que o fax seja enviado para o atacante que está em outro número.

Uso do voice mail

14-1 Senhas de voice mail

Política: As senhas de voice mail nunca devem ser divulgadas para ninguém sob nenhum pretexto. Além disso, elas devem ser alteradas a cada 90 dias ou menos,

Explicação/Observações: As informações confidenciais da empresa podem ser deixadas nas mensagens do voice mail. Para proteger essas informações, os empregados devem alterar suas senhas com freqüência e nunca devem divulgá-las. Além disso, não devem usar senhas iguais ou semelhantes em um período de 12 meses.

14-2 Senhas em diversos sistemas

Política: Os usuários de voice mail não devem usar a mesma senha em qualquer outro telefone ou sistema de computador, seja ele interno ou externo à empresa.

Explicação/Observações: O uso de uma senha semelhante ou idêntica em diversos dispositivos, tais como um voice mail e um computador, facilita a adivinhação de todas as senhas de um usuário após a identificação de apenas uma.

14-3 Definindo as senhas de voice mail

Política: Os usuários e os administradores de voice mail devem criar senhas de voice mail que sejam difíceis de adivinhar. Elas não devem estar relacionadas de nenhuma maneira com a pessoa que as usa nem com a empresa e não devem conter um padrão previsível que pode ser adivinhado facilmente.

Explicação/Observações: As senhas não devem conter dígitos seqüenciais ou repetidos (ou seja, 1111, 1234, 1010), não podem ser iguais ou baseadas no número do ramal de telefone e não devem estar relacionadas com endereço, código postal, data de nascimento, placas de carro, número de telefone, peso, Q.I. ou outras informações pessoais previsíveis.

14-4 Mensagens de correio eletrônico marcadas como "antigas"

Política: Quando as mensagens de correio eletrônico que ainda não foram ouvidas não estão marcadas como mensagens novas, o administrador do voice mail deve ser notificado sobre uma possível violação da segurança e a senha do voice mail deve ser imediatamente alterada.

Explicação/Observações: Os engenheiros sociais podem ter acesso a uma caixa postal de voice mail de várias maneiras. Um empregado que descobre que as mensagens que ele nunca ouviu não estão sendo anunciadas como mensagens novas deve supor que outra pessoa obteve acesso autorizado à caixa postal do voice mail e ouviu as mensagens.

14-5 Cumprimentos no voice mail externo

Política: Os funcionários da empresa devem limitar a divulgação de informações em seu cumprimento externo no voice mail. Geralmente as informações relacionadas com rotina diária de um funcionário ou a sua programação de viagens não devem ser divulgadas.

Explicação/Observações: Um cumprimento externo (reproduzido para as pessoas de fora) não deve incluir o sobrenome, o ramal ou o motivo da ausência (tal como viagem, férias ou itinerário diário). Um atacante pode usar essas informações para desenvolver uma história plausível em sua tentativa de enganar os outros funcionários.

14-6 Padrões de senha de voice mail

Política: Os usuários do voice mail não devem selecionar uma senha na qual uma parte permanece fixa, enquanto a outra parte muda de acordo como um padrão previsível.

Explicação/Observações: Por exemplo, não use uma senha tal como 743501, 743502, 743503 e assim por diante, na qual os dois últimos dígitos correspondem ao mês atual.

14-7 Informações confidenciais ou particulares

Política: As informações Confidenciais ou Particulares não devem ser divulgadas em uma mensagem de voice mail.

Explicação/Observações: O sistema corporativo de telefones via de regra é mais vulnerável do que os sistemas corporativos de computadores. As senhas em geral são uma string de dígitos, o que limita o número de possibilidades que um atacante tem para adivinhar. Além disso, em algumas organizações, as senhas de voice mail podem ser compartilhadas com secretárias ou outras pessoas da equipe administrativa que têm a responsabilidade de receber recados para seus gerentes. Tendo isso em vista, nenhuma informação Sigilosa deve ser deixada no voice mail de alguém.

Senhas

15-1 Segurança do telefone

Política: As senhas não devem ser divulgadas ao telefone em nenhum momento.

Explicação/Observações: Os atacantes podem encontrar maneiras de ouvir as conversações telefônicas, seja pessoalmente ou por meio de um dispositivo tecnológico.

1 5-2 Revelando as senhas de computador

Política: Sob nenhuma circunstância um usuário de computador deve revelar sua senha para ninguém sem antes obter o consentimento por escrito do gerente responsável pela tecnologia da informação.

Explicação/Observações: O objetivo de muitos ataques da engenharia social é enganar pessoas inocentes para que elas revelem os nomes e as senhas de suas contas. Esta política é uma etapa importante para reduzir o risco de que os ataques da engenharia social contra a empresa sejam bem-sucedidos. Sendo assim, ela precisa ser seguida religiosamente em toda a empresa.

1 5-3 Senhas da Internet

Política: O pessoal nunca deve usar uma senha que seja igual ou semelhante àquela que estão usando em qualquer sistema corporativo de um site da Internet.

Explicação/Observações: Os operadores maliciosos de sites Web podem configurar um site que diz oferecer algo de valor ou a possibilidade de ganhar um prêmio. Para se registrar, o visitante do site deve inserir um endereço de correio eletrônico, um nome de usuário e uma senha. Como muitas pessoas usam informações iguais ou semelhantes de forma repetida, o operador malicioso do site Web tentará usar a senha escolhida e as suas variações para atacar o sistema de computadores no trabalho ou na casa do alvo. O computador de trabalho do visitante às vezes pode ser identificado pelo endereço de correio eletrônico inserido durante o processo de registro.

1 5-4 Senhas em diversos sistemas

Política: Os funcionários nunca devem usar uma senha igual ou semelhante em mais de um sistema. Esta política diz respeito a diversos tipos de dispositivos (computador ou voice mail), a diversas localizações de dispositivos (em casa ou no trabalho) e a diversos tipos de sistemas, dispositivos (roteador ou firewall) ou programas (banco de dados ou aplicativo).

Explicação/Observações: Os atacantes usam determinadas características da natureza humana para invadir os sistemas e as redes de computadores. Eles sabem que para evitar o embaraço de controlar diversas senhas, muitas pessoas usam senhas iguais ou semelhantes em todos os sistemas que acessam. Assim sendo, o intruso tentará aprender a senha de um sistema no qual o alvo tenha uma conta. Após obtê-la, é muito provável que essa senha ou uma variação dela dê o acesso aos outros sistemas e dispositivos usados pelo empregado.

1 5-5 Reutilizando as senhas

Política: Nenhum usuário de computador deve usar uma senha igual ou semelhante dentro do mesmo período de 18 meses.

Explicação/Observação: Se um atacante descobrir a senha de um usuário, a mudança freqüente da senha minimiza o dano que pode ser causado. Criar uma senha nova que seja diferente da anterior é algo que torna mais difícil a sua adivinhação pelo atacante.

1 5-6 Padrões de senhas

Política: Os empregados não devem selecionar uma senha na qual uma parte permanece fixa e o outro elemento muda seguindo um padrão previsível.

Explicação/Observações: Por exemplo, não use uma senha tal como Kevin0l, Kevin02. Kevin03 e assim por diante, na qual os dois últimos dígitos correspondem ao mês atual.

1 5-7 Selecionando as senhas

Política: Os usuários de computadores devem criar ou selecionar senhas que sigam os requisitos a seguir:

- Tenham pelo menos oito caracteres de comprimento para as contas padrão de usuários e pelo menos 12 caracteres de comprimento para as contas com privilégios.
- Contenham pelo menos um número, pelo menos um símbolo (tal como $, _, !. *&)*. pelo menos uma letra minúscula e pelo menos uma letra maiúscula (na medida em que tais variáveis sejam suportadas pelo sistema operacional).

- Não sejam nenhum destes itens: palavras de um dicionário de qualquer idioma; qualquer palavra que esteja relacionada com família, hobbies, veículo, trabalho, placas do veículo. número de seguro social, endereço, telefone, nome do bichinho de estimação do empregado ou frases contendo essas palavras.
- Não sejam a variação de uma senha usada anteriormente com um elemento que permanece o mesmo e outro que muda, tal como kevin, kevin1, kevin2 ou kevinjan, kevinfev.

Explicação/Observações: Esses parâmetros produzem uma senha que é difícil de ser adivinhada pelo engenheiro social. Outra opção é o método da consoante e vogai, o qual fornece uma senha fácil de lembrar e de ser pronunciada. Para criar esse tipo de senha substitua as consoantes pela letra C e as vogais pela letra V usando a máscara de "CVCVCVCV". Os exemplos incluem MIXOCASO; CUSOJENA.

1 5-8 Escrevendo as senhas

Política: Os empregados devem escrever as senhas apenas quando forem armazenadas em uma localização distante do computador ou de outro dispositivo protegido por senha.

Explicação/Observações: Os empregados não devem nunca escrever as senhas. Em determinadas condições, porém, isso pode ser necessário, por exemplo, no caso de um empregado que tem diversas contas em diferentes sistemas de computadores. Todas as senhas escritas devem estar seguras em um local longe do computador. Sob nenhuma circunstância uma senha pode ser armazenada sob o teclado ou pregada no monitor do computador.

1 5-9 Senhas em texto simples nos arquivos do computador

Política: As senhas em texto simples não devem ser salvas em nenhum arquivo de computador, nem devem ser armazenadas como texto que pode ser chamado com uma tecla de função. Quando for preciso, as senhas podem ser salvas usando-se um utilitário de criptografia aprovado pelo departamento de TI para evitar a divulgação não autorizada.

Explicação/Observações: As senhas podem ser recuperadas facilmente por um atacante se elas forem armazenadas na forma não criptografada em arquivos de dados de computador, arquivos de lote, teclas de função do terminal, arquivos de login, macro ou programas de scripting ou em quaisquer arquivos de dados que contenham senhas de sites FTP.

POLÍTICAS PARA OS TELECOMUTADORES

Os telecomutadores estão fora do firewall corporativo e, portanto, estão mais vulneráveis a um ataque. Estas políticas ajudam a evitar que os engenheiros sociais usem os seus empregados telecomutadores como uma porta de entrada para os seus dados.

16-1 Clientes Thin

Política: Todo o pessoal da empresa que foi autorizado a se conectar via acesso remoto deve usar um thin client para se conectar à rede corporativa.

Explicação/Observações: Quando um atacante analisa uma estratégia de ataque, ele tenta identificar os usuários que acessam a rede corporativa de localizações externas. Como tal, os teleco-

mutadores são os alvos primários. Seus computadores têm menos chances de ser rigidamente controlados e podem ser um elo fraco que comprometa a rede corporativa.

Todo computador que se conecta a uma rede segura pode ser invadido por meio das teclas digitadas ou sua conexão autenticada pode ser seqüestrada. Uma estratégia de cliente thin pode ser usada para evitar problemas. Um cliente thin é como uma estação de trabalho sem disco ou um terminal burro. O computador remoto não tem capacidades de armazenamento, mas o sistema operacional, os programas de aplicativos e os dados residem todos na rede corporativa. O acesso da rede por meio de um cliente thin diminui substancialmente o risco dos sistemas sem patch, dos sistemas operacionais desatualizados e do código malicioso.

Da mesma forma, o gerenciamento da segurança dos telecomutadores é efetivo e mais fácil pela centralização dos controles de segurança. Em vez de usar o telecomutador inexperiente para gerenciar adequadamente as questões relacionadas com segurança, essas responsabilidades são deixadas para os administradores treinados de sistema, rede ou segurança.

16-2 Software de segurança para os sistemas de computador de telecomutador

Política: Todo sistema externo de computadores que é usado para a conexão com a rede corporativa deve ter software antivírus, software que o proteja do Cavalo de Tróia e um firewall pessoal (hardware ou software). Os arquivos de definições do antivírus ou do Cavalo de Tróia precisam ser atualizados pelo menos uma vez por semana.

Explicação/Observações: Normalmente, os telecomutadores não são treinados nas questões relacionadas com segurança e podem, sem querer ou por negligência, deixar seus sistemas de computadores e a rede corporativa abertos para o ataque. Os telecomutadores, portanto, representam um sério risco para a segurança se não forem bem treinados. Além da instalação de software antivírus e contra o Cavalo de Tróia para protegê-los do código malicioso, um firewall é necessário para impedir que todos os usuários hostis obtenham o acesso a quaisquer serviços ativados no sistema do telecomutador.

O risco de não empregar as tecnologias de segurança mínimas para evitar que o código malicioso se propague não pode ser subestimado, como mostra um ataque realizado contra a Microsoft. Um sistema de computador pertencente a um telecomutador da Microsoft e usado para se conectar à rede corporativa da Microsoft foi infectado com um programa Cavalo de Tróia. O intruso ou os intrusos puderam usar a conexão segura do telecomutador com a rede de desenvolvimento da Microsoft para roubar código-fonte de desenvolvimento.

POLÍTICAS PARA RECURSOS HUMANOS

Os departamentos de recursos humanos têm a responsabilidade especial de proteger os empregados contra as pessoas que tentam descobrir informações pessoais por intermédio do seu local de trabalho. Os profissionais de RH também têm a responsabilidade de proteger sua empresa contra as ações de ex-empregados descontentes.

17-1 Empregados demitidos

Política: Sempre que uma pessoa empregada pela empresa sai ou é demitida, o departamento de Recursos Humanos deve imediatamente tomar estas medidas:

- Remover o nome da pessoa da lista de telefones on-line de empregados e desativar ou redirecionar seu voice mail.
- Notificar o pessoal das portarias do prédio ou dos saguões da empresa.
- Incluir o nome do empregado na lista de empregados demitidos, a qual deve ser enviada por correio eletrônico para todo o pessoal com uma freqüência não inferior a uma vez por semana.

Explicação/Observações: Os empregados que ficam nas entradas do prédio devem ser notificados a não deixar que um ex-empregado entre novamente nas instalações. Além disso, a notificação das outras pessoas pode evitar que o ex-empregado faça-se passar por um empregado legitimo e engane o pessoal para que tomem alguma ação que possa causar danos à empresa.

Em algumas circunstâncias, talvez seja preciso exigir que cada usuário dentro do departamento do ex-empregado mude a sua senha. (Quando fui demitido da GTE apenas por causa da minha reputação de hacker, a empresa exigiu que todos os empregados de toda a empresa mudassem suas senhas.)

1 7-2 Notificação ao departamento de TI

Política: Sempre que uma pessoa empregada pela empresa sai ou é demitida, o departamento de Recursos Humanos deve notificar imediatamente o departamento de tecnologia da informação para desativar as contas de computador do ex-empregado, incluindo todas as contas usadas para o acesso a bancos de dados, discagem ou acesso à Internet de localizações remotas.

Explicação/Observações: É essencial que todo o acesso do ex-funcionário a todos os sistemas de computadores, dispositivos de rede, bancos de dados ou quaisquer outros dispositivos relacionados com computador sejam imediatamente desativados após o seu desligamento. Caso contrário, a empresa pode deixar a porta aberta para que um empregado insatisfeito acesse os sistemas de computadores da empresa e cause danos significativos.

1 7-3 Informações confidenciais usadas no processo de contratação

Política: Os anúncios e as outras formas de solicitação pública de candidatos para o preenchimento de vagas devem, na medida do possível, evitar a identificação do hardware e software de computador usado pela empresa.

Explicação/Observações: Os gerentes e o pessoal de recursos humanos só devem divulgar as informações relacionadas com o hardware e software de computador da empresa que sejam relativamente necessárias para obter os currículos dos candidatos qualificados.

Os atacantes lêem os jornais e os press releases das empresas e visitam os sites na Internet para encontrar as listagens de cargos. Quase sempre, as empresas divulgam muitas informações sobre os tipos de hardware e software usados para atrair possíveis empregados. Após o intruso descobrir os sistemas de informações do alvo, ele está preparado para a próxima fase do ataque. Por exemplo, sabendo que determinada empresa usa o sistema operacional VMS. o atacante pode fazer ligações para determinar a versão e, em seguida, pode enviar um patch de segurança de emergência falso feito para parecer que veio do desenvolvedor do software. Depois que o patch está instalado, o atacante está dentro da empresa.

1 7-4 Informações pessoais de empregado

Política: O departamento de recursos humanos nunca deve liberar informações pessoais sobre nenhum empregado atual ou ex-empregado, contratado, consultor, funcionário temporário ou esta-

giário, exceto com o consentimento prévio, expresso e por escrito do empregado ou do gerente de recursos humanos.

Explicação/Observações: Os head-hunters, detetives particulares e ladrões de identidade visam as informações particulares dos empregados, tais como número de empregado, número de seguro social, data de nascimento, histórico de salário, dados financeiros, incluindo as informações de depósito e informações relacionadas com benefícios de saúde. O engenheiro social pode obter essas informações para se fazer passar pelo indivíduo. Além disso, a divulgação dos nomes dos novos contratados pode ser muito valiosa para os ladrões de informações. Os novos contratados podem atender a qualquer solicitação feita por pessoas com grau mais alto ou em posição de autoridade ou por qualquer pessoa que alegue ser da segurança corporativa.

1 7-5 Verificação de antecedentes

Política: Uma verificação de antecedência deve ser feita para todos os novos contratados, consultores, funcionários temporários, contratados ou estagiários antes de uma oferta de emprego ou de um relacionamento com contrato.

Explicação/Observações: Devido às questões de custo, as verificações de antecedentes podem ser limitadas a posições de confiança específicas. Observe, porém, que qualquer pessoa que recebe o acesso físico aos escritórios corporativos pode ser uma ameaça em potencial. Por exemplo, as equipes de limpeza transitam nos escritórios do pessoal, o que lhes dá o acesso a quaisquer sistemas de computadores localizados neles. Um atacante que tenha o acesso físico a um computador pode instalar um *keylogger* (detector de teclas digitadas) em menos de um minuto para capturar as senhas.

Os intrusos de computador às vezes se dão ao trabalho de obter um emprego como um meio de ter acesso aos sistemas e redes de computadores de uma empresa-alvo. Um atacante pode obter facilmente o nome da empresa de limpeza contratada por uma companhia ligando para o empregado responsável na companhia-alvo, alegando ser de uma empresa de limpeza que está procurando clientes e, em seguida, obtendo o nome da empresa que no momento fornece esses serviços.

POLÍTICAS PARA A SEGURANÇA FÍSICA

Embora os engenheiros sociais tentem evitar aparecer pessoalmente em um local de trabalho que é o seu alvo, existem ocasiões em que eles violam esse espaço. Estas políticas ajudam você a manter as suas instalações físicas seguras contra essa ameaça.

18-1 Identificação para não-empregados

Política: O pessoal de entrega e outros não-empregados que precisam entrar nas instalações da empresa regularmente devem ter um crachá especial ou outra forma de identificação de acordo com a política estabelecida pela segurança corporativa.

Explicação/Observações: Os não-empregados que precisam entrar no prédio regularmente (por exemplo, para fazer entregas de alimentos ou bebidas no restaurante ou para consertar máquinas copiadoras e instalar telefones) devem ter um crachá de identificação da empresa que c usado para essa finalidade.

As outras pessoas que precisam entrar apenas eventualmente ou uma só vez devem ser tratadas como visitantes e devem estar sempre acompanhadas.

1 8-2 Identificação de visitante

Política: Todos os visitantes devem apresentar uma carteira de identidade válida ou outra identificação com foto para serem admitidos nas instalações da empresa.

Explicação/Observações: A equipe de segurança ou recepção deve fazer uma fotocópia do documento de identificação antes de emitir um crachá de visitante. A cópia deve ser mantida com o registro do visitante. As informações de identificação também podem ser registradas no livro de visitantes pela recepção ou pelo guarda; os visitantes não podem escrever suas próprias informações de identificação.

Os engenheiros sociais que querem entrar em um prédio sempre escrevem informações falsas no registro. Embora não seja difícil obter um ID falso e descobrir o nome de um empregado que podem estar visitando, a exigência de que o empregado responsável registre a entrada inclui um nível extra de segurança no processo.

1 8-3 Acompanhamento de visitantes •

Política: O visitante deve ser acompanhado ou estar na companhia de um empregado durante todo o tempo.

Explicação/Observações: Um truque conhecido dos engenheiros sociais é conseguir uma visita a um empregado da empresa (por exemplo, a visita a um engenheiro de produto sob o pretexto de ser o empregado de um parceiro estratégico). Após ser acompanhado para a reunião principal, o engenheiro social garante ao empregado que ele consegue encontrar o caminho de volta até a recepção. Assim ele ganha a liberdade para perambular pelo prédio e possivelmente ter acesso a informações Sigilosas.

1 8-4 Crachás temporários

Política: Os funcionários de outra localização que não têm seus crachás de identificação devem apresentar uma carteira de identidade válida ou outro documento com foto e receber um crachá temporário de visitante.

Explicação/Observações: Quase sempre, os atacantes fazem-se passar por empregados de um escritório ou filial diferente para ter acesso a uma empresa.

1 8-5 Evacuação de emergência

Política: Em uma situação de emergência ou simulação, o pessoal da segurança deve garantir que todos tenham saído das instalações.

Explicação/Observações: O pessoal da segurança deve verificar se alguma pessoa ficou nos banheiros ou nas áreas de escritórios. Conforme autorização da Brigada de Incêndio ou de outra autoridade responsável, a equipe de segurança precisa estar alerta para todos aqueles que saem do prédio muito depois da sua evacuação.

Os espiões industriais ou atacantes podem criar uma distração para ter acesso a um prédio ou área segura. Uma das distrações usadas é lançar no ar um produto químico inofensivo chamado butil

mercaptano. O efeito dá a impressão de que há um vazamento de gás natural. Depois que o pessoal inicia os procedimentos de evacuação, o audacioso atacante usa esse truque para roubar informações ou ter acesso aos sistemas de computadores da empresa. Outra tática usada pelos ladrões de informações é ficar para trás, em banheiros ou armários, no momento de uma simulação programada de evacuação do prédio, ou após criar uma fumaça falsa ou outro dispositivo para causar uma evacuação de emergência.

1 8-6 Visitantes da sala de correspondência

Política: Nenhum visitante pode entrar na sala de correspondência sem a supervisão de um funcionário da empresa.

Explicação/Observações: A intenção desta política é evitar que um estranho troque, envie ou roube correspondência interna da empresa.

1 *8-7* Números das placas de veículos

Política: Se a empresa tiver uma área de estacionamento com guardas, a equipe de segurança deve registrar os números das placas de todos os veículos que entram na área.

1 8-8 Contêineres de lixo

Política: Os contêineres de lixo devem sempre permanecer nas instalações da empresa e não podem ser acessados pelo público.

Explicação/Observações: Os atacantes e os espiões industriais podem obter informações valiosas nas latas de lixo da empresa. A justiça considera que o lixo é encarado legalmente como propriedade abandonada, de modo que o ato de *virar latas é* perfeitamente legal, desde que os depósitos de lixo estejam em propriedade pública. Por esse motivo é importante que os depósitos de lixo estejam situados na propriedade da empresa, onde ela tem o direito legal de proteger os contêineres e seu conteúdo.

POLÍTICAS PARA RECEPCIONISTAS

Os recepcionistas quase sempre estão na linha de frente no que diz respeito a lidar com os engenheiros sociais, mas eles raramente têm um treinamento suficiente em segurança para reconhecer e deter um invasor. Institua estas políticas para ajudar o seu recepcionista a proteger melhor a sua empresa e seus dados.

19-1 Diretório interno

Política: A divulgação das informações do diretório interno da empresa deve ser limitada às pessoas empregadas pela empresa.

Explicação/Observações: Todos os cargos, nomes, números de telefone e endereços de empregados contidos no diretório da empresa devem ser considerados informações Internas, e só devem ser divulgados de acordo com a política relacionada com classificação de dados e informações internas.

Além disso, toda pessoa que liga deve ter o nome e o ramal da pessoa que está tentando contatar. Embora o recepcionista possa fazer uma transferência de ligação quando um interlocutor não sabe

o número do ramal, a divulgação do número do ramal para o interlocutor deve ser proibida. (Para aquele pessoal curioso que só acredita vendo: experimente este procedimento ligando para a Agência Nacional de Segurança e pedindo ao telefonista o número de um ramal.)

19-2 Números de telefone para departamentos/grupos específicos

Política: Os empregados não devem fornecer números diretos de telefone do help desk da empresa, do departamento de telecomunicações, de operações de computadores ou do pessoal da administração de sistemas sem antes verificar se o solicitante tem uma necessidade legítima de entrar em contato com esses grupos. Ao transferir a ligação para esses grupos, o recepcionista deve anunciar o nome de quem está ligando.

Explicação/Observações: Embora algumas organizações achem esta política restritiva, esta regra torna ainda mais difícil para um engenheiro social disfarçar-se de empregado e fazer os outros empregados transferirem a ligação de seus ramais (o que em alguns sistemas de telefone faz com que a ligação pareça se originar de dentro da empresa) ou demonstrar conhecimento desses ramais para a vítima a fim de criar uma idéia de autenticidade.

19-3 Retransmitindo informações

Política: Os operadores de telefone e recepcionistas não devem anotar recados ou passar mensagens por parte de qualquer pessoa que não seja conhecida pessoalmente como um empregado.

Explicação/Observações: Os engenheiros sociais gostam de enganar os empregados para que eles endossem sem querer a sua identidade. Um truque da engenharia social é obter o número de telefone da recepcionista e, com algum pretexto, pedir que ela anote todos os recados que sejam deixados para ele. Em seguida, durante uma ligação para a vítima, o atacante finge ser um empregado, pede algumas informações sigilosas ou pede para ela executar uma tarefa e dá o número do PBX como um número de retomo. Mais tarde o atacante liga de volta para a recepcionista e recebe a mensagem que foi deixada para ele pela vítima desavisada.

1 9-4 Itens deixados para retirada

Política: Antes de liberar qualquer item para um mensageiro ou outra Pessoa Não Verificada, a recepcionista ou o guarda de segurança deve obter uma identificação com foto e registrar as informações de identificação no registro de retiradas de acordo com os procedimentos aprovados.

Explicação/Observações: Uma tática da engenharia social é enganar um empregado para que ele libere material sigiloso para outro empregado supostamente autorizado, deixando tal material na recepção ou no saguão para retirada. Naturalmente, a recepcionista ou guarda de segurança supõe que o pacote pode ser retirado. O engenheiro social vai pessoalmente ou manda um serviço de mensageiros retirar o pacote.

POLÍTICAS PARA O GRUPO RESPONSÁVEL PELOS INCIDENTES DE SEGURANÇA

Toda empresa deve definir um grupo centralizado que seja notificado quando alguma forma de ataque à segurança corporativa for identificada. A seguir temos algumas orientações para definir e estruturar as atividades desse grupo.

20-1 Grupo responsável pelos incidentes de segurança

Política: Um indivíduo ou grupo deve ser designado e os empregados devem ser instruídos para relatar os incidentes de segurança para esse indivíduo ou grupo. Todos os empregados devem receber as informações de contato com o grupo.

Explicação/Observações: Os empregados devem saber como identificar uma ameaça à segurança e devem ser treinados para relatar toda ameaça a um grupo responsável pelos incidentes de segurança específico. Também é importante que uma organização estabeleça procedimentos e autoridade específicos para que tal grupo possa agir quando uma ameaça for detectada.

20-2 Ataques em andamento

Política: Sempre que o grupo responsável pelos incidentes de segurança receber os relatórios de um ataque de engenharia social, ele deve iniciar imediatamente os procedimentos para alertar todos os empregados dos grupos-alvo.

Explicação/Observações: O grupo em questão ou o gerente responsável também devem enviar um alerta para toda a empresa. Após a pessoa ou o grupo responsável estar convencido de que pode estar acontecendo um ataque, a diminuição do dano deve ser a prioridade, e o pessoal da empresa deve ser notificado para estar alerta.

Um exame rápido da segurança

As listagens e os quadros a seguir fornecem um guia de referência rápida para os métodos da engenharia social discutidos nos Capítulos 2 a 14 e para os procedimentos de verificação detalhados no Capítulo 16. Adeqüe estas informações à sua organização e torne-as disponíveis para que os empregados as consultem quando surgir uma dúvida sobre a segurança da informação.

IDENTIFICAÇÃO DE UM ATAQUE À SEGURANÇA

Estas tabelas e listas de verificação o auxiliam a detectar um ataque da engenharia social.

O ciclo da engenharia social

AÇÃO	DESCRIÇÃO
Pesquisa	Pode incluir informações públicas, tais como arquivos e relatórios anuais da SEC, documentos de marketing, aplicações de patente, recortes de jornais, revistas da indústria, conteúdo de sites Web. Também chamado de Virar latas.
Desenvolvimento da credibilidade e da confiança	Usa as informações internas, finge ser outra pessoa, cita pessoas conhecidas da vítima, busca ajuda ou autoridade.
Explorando a confiança	Solicita informações ou ações por parte da vítima. Inversamente, manipula a vítima para que ela peça ajuda ao atacante.
Utilização das informações	Se as informações obtidas são apenas uma etapa para o objetivo final, o atacante retorna às etapas anteriores do ciclo até que o objetivo seja atingido.

Métodos comuns da engenharia social

- Finge ser um colega de trabalho
- Finge ser um empregado de um fornecedor, empresa parceira ou autoridade legal
- Finge ser alguém com autoridade
- Finge ser um empregado novo que solicita ajuda

- Finge ser um fornecedor ou fabricante de sistemas que liga para oferecer um patch ou uma atualização de sistema
- Oferece ajuda quando ocorrer um problema e, em seguida, faz o problema ocorrer para manipular a vítima e fazer com que ela ligue pedindo ajuda
- Envia software ou patch grátis para que a vitima o instale
- Envia um vírus ou Cavalo de Tróia como um anexo de correio eletrônico
- Usa uma janela pop-up falsa que pede para o usuário fazer o login novamente ou digitar uma senha
- Captura as teclas digitadas pela vítima com um sistema ou programa de computador
- Deixa um disquete ou CD com software malicioso em algum lugar do local de trabalho
- Usa jargão e terminologia interna para ganhar a confiança
- Oferece um prêmio pelo registro em um site Web com um nome de usuário e a senha
- Deixa um documento ou arquivo na sala de correspondência para entrega interna
- Modifica o cabeçalho de uma máquina de fax para que ele venha de uma localização interna
- Pede que uma recepcionista receba e, em seguida, encaminhe um fax
- Pede que um arquivo seja transferido para uma localização aparentemente interna
- Configura uma caixa de correio para que as ligações de retorno percebam o atacante como alguém de dentro da empresa
- Finge ser do escritório remoto e pede acesso local ao correio eletrônico

Sinais de um ataque

- Recusa em dar um número de retorno
- Solicitação fora do comum
- Alegação de autoridade
- Ênfase na urgência
- Ameaça de conseqüências negativas em caso de não atendimento
- Mostra desconforto quando questionado
- Nome falso
- Cumprimentos ou lisonja
- Flerte

Alvos comuns dos ataques

TIPO DE ALVO	EXEMPLOS
Desconhecimento do valor das informações de	Recepcionistas, telefonistas, assistentes administrativos, guardas segurança.
Privilégios especiais	Help desk ou suporte técnico, administradores de sistema, operadores de computador, administradores do sistema de telefones.

Fabricante/fornecedor	Hardware de computador, fabricantes de software, fornecedores de sistemas de voice mail.
Departamentos específicos	Contabilidade, recursos humanos.

Fatores que tornam as empresas mais vulneráveis aos ataques

- Um número grande de empregados
- Diversas instalações
- Informações sobre o paradeiro dos empregados deixadas nas mensagens de voice mail
- Informações de ramal de telefone disponíveis
- Falta de treinamento em segurança
- Falta de sistema de classificação de dados
- Nenhum plano ou grupo de resposta aos incidentes de segurança

VERIFICAÇÃO E CLASSIFICAÇÃO DE DADOS

Estas tabelas e gráficos o ajudam a responder às solicitações de informações ou ações que podem ser ataques da engenharia social.

Verificação de procedimento de identidade

AÇÃO	DESCRIÇÃO
ID de chamadas	Verifica se a ligação e interna e se o nome e número do ramal coincidem com a identidade do interlocutor.
Retorno de ligação (Callback)	Procura o solicitante no diretório da empresa e liga de volta para o ramal relacionado.
Endosso	Pede para um empregado de confiança endossar a identidade do solicitante.
Segredo comum compartilhado	Solicita um segredo compartilhado da empresa, tal como uma senha ou código diário.
Supervisor ou gerente	Contata o supervisor imediato do empregado e solicita a verificação da identidade e do status de emprego.
Correio eletrônico seguro	Solicita uma mensagem assinada digitalmente.
Reconhecimento pessoal de voz	Para um interlocutor conhecido do empregado, validado pela voz do interlocutor.
Senhas dinâmicas	Verifica com relação a uma solução de senha dinâmica, tal como um ID Seguro ou outro dispositivo de autenticação segura.
Pessoalmente	Exige que o solicitante apareça pessoalmente com um crachá de empregado ou outra identificação.

Procedimento de verificação de status no trabalho

AÇÃO	DESCRIÇÃO
Verificação no diretório de empregados	Verifica se o solicitante está relacionado no diretório *on-line.*
Verificação do gerente do solicitante	Ligação para o gerente do solicitante usando o número de telefone relacionado no diretório da empresa.
Verificação do departamento OU grupo de trabalho do solicitante	Ligação para o departamento ou grupo de trabalho do solicitante para determinar se ele ainda é empregado da empresa.

Procedimento para determinar a necessidade de conhecimento das informações

AÇÃO	DESCRIÇÃO
Consultar a lista de responsabilidades do cargo/grupo de trabalho	Verificar nas listas publicadas quais empregados têm direito de receber as informações confidenciais específicas.
Obter autorização do gerente	Entrar em contato com o seu gerente, ou com o gerente do solicitante, para obter a autorização para atender à solicitação.
Obter autorização do Proprietário das informações ou representante	Perguntar ao Proprietário das informações se o solicitante tem necessidade de conhecê-las.
Obter a autorização com uma ferramenta automatizada	Verificar o banco de dados proprietário de pessoal autorizado.

Critérios para a verificação de não-empregados

CRITÉRIO	AÇÃO
Relacionamento	Verificar se a empresa do solicitante tem um relacionamento de fornecedor, parceiro estratégico ou outro.
Identidade	Verificar a identidade do solicitante e o status de emprego na empresa do fornecedor/parceiro.
Confidencialidade	Verificar se o solicitante assinou um contrato de confidencialidade que está arquivado.
Acesso	Encaminhar a solicitação para o gerenciamento quando as informações tiverem classificação acima de Internas.

Classificação de dados

CLASSIFICAÇÃO	DESCRIÇÃO	PROCEDIMENTO
Público	Pode ser liberado para o público.	Não há necessidade de verificação.

CLASSIFICAÇÃO	DESCRIÇÃO	PROCEDIMENTO
Interno	Para uso dentro da empresa.	Verificar a identidade do solicitante como um empregado ativo ou verificar o contraio de confidencialidade em arquivo e pedir aprovação do gerenciamento para não-empregados.
Particular	As informações de natureza pessoal destinadas ao uso apenas dentro da empresa.	Verificar a identidade do solicitante como um empregado ativo ou não empregado com autorização. Consultar o departamento de recursos humanos antes de divulgar informações Particulares para empregados autorizados ou solicitantes externos.
Confidencial	Compartilhados apenas com o pessoal que tem necessidade absoluta de conhecer as informações dentro da organização.	Verificar a identidade do solicitante e a necessidade de conhecê-las do Proprietário designado das informações. Liberar apenas com consentimento prévio, por escrito, do gerente ou do Proprietário das informações ou seu representante. Verificar o contrato de confidencialidade em arquivo. Apenas o pessoal do gerenciamento pode divulgar para as pessoas não-empregadas pela empresa.

Respondendo a uma solicitação de informações

As Perguntas de Ouro

Como sei que esta pessoa é quem ela diz ser?
Como sei que esta pessoa tem autoridade para fazer a solicitação?

Solicita informações sobre...

EXEMPLOS

Exemplos	Solicita informações sobre...	Sim
	Quaisquer senhas	NUNCA divulgar a sua senha sob nenhuma circunstância.
Estrutura hierárquica do pessoal, nomes e cargos dos empregados.	Não → Detalhes do quadro organizacional	Seguir os procedimentos para divulgação das informações internas.
Números de telefones internos designados à equipe, números de fax internos, números internos do prédio e listas departamentais.	Não → Listas de telefone/diretório da empresa	Seguir os procedimentos para a divulgação de informações internas.
Números pessoais de telefone (residencial ou celular), número do seguro social, endereço residencial, histórico de empregos anteriores e salários.	Não → Informações pessoais	Seguir os procedimentos para a divulgação de informações internas.
Tipo de sistema operacional, procedimentos *de* acesso remoto, números de discagem e nomes designados aos sistemas de computadores.	Não → Procedimento ou informações sobre o sistema de computadores.	Seguir os procedimentos para a divulgação de informações internas.
Processos de manufatura, planos estratégicos, código-fonte proprietário, listas de clientes e segredos comerciais.	Não → Informações confidenciais ou particulares	Determinar a classificação dos dados; seguir os procedimentos apropriados para a divulgação.

Todas as informações são consideradas sigilosas, a menos que sejam designadas especificamente para a divulgação ao público.

Respondendo a uma solicitação de informações

As Perguntas de Ouro

Não confiar em ninguém sem verificação.
O questionamento das solicitações é encorajado.

Solicita ação relativa a ...

OBSERVAÇÕES

Abrir anexo de correio eletrônico — Sim → Não abrir anexos, a menos que a mensagem já seja esperada; examinar todos os anexos com software antivírus.

Não

Alterar a sua senha — Sim → NUNCA altere a sua senha para algo que outra pessoa conhece, mesmo que seja por alguns instantes.

Não

Transferência eletrônica de informações internas — Sim → Determinar a classificação dos dados; seguir os procedimentos adequados de divulgação.

Código-fonte proprietário, segredos comerciais, processo de manufatura, fórmulas, especificações de produto, dados de marketing ou planos de negócios.

Não

Inserir comandos em qualquer computador — Sim → O solicitante deve ser apenas do departamento de TI; consulte os Procedimentos de Verificação de Empregados.

Nunca digitar comandos desconhecidos ou executar programas sob solicitação de qualquer pessoa, a menos que isso seja especificamente aprovado pelo departamento de TI.

Não

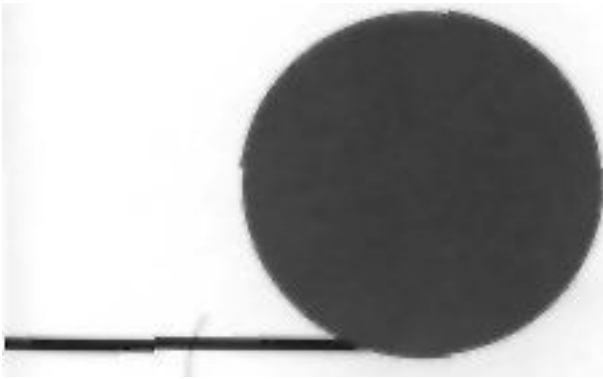
Download, instalação, remoção ou desativamento de qualquer software — Sim → O solicitante deve ser apenas do departamento de TI; consulte os Procedimentos de Verificação de Empregados.

Instalar software apenas de fontes confiáveis que possam ser autenticadas por assinatura digital.

Não

Alterar as definições do sistema/rede de computador — Sim → O solicitante deve ser apenas do departamento de TI; consulte os Procedimentos de Verificação de Empregados.

Não altere nenhuma definição da BIOS do sistema operacional ou de qualquer aplicativo (incluindo o firewall pessoal ou os utilitários de antivírus), a menos que isso seja especificamente aprovado pelo departamento de TI.

Todas as ações que você realiza a pedido de outras pessoas podem resultar em comprometimento dos bens da sua empresa. Verifique. Verifique. Verifique,

Fontes

CAPÍTULO 1

BLOOMBECKER, Buck. *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year* Irwin Professional Publishing, 1990.

LITTMAN. Jonathan. *The Fugitíve Game: Online with Kevin Mitnick.* Little Brown & Co, 1997.

PENENBERG, Adam L. "The Demonizing of a Hacker." Forbes, 19 abr. 1999.

CAPÍTULO 2

A história de Stanley Rifkin baseada nestes relatos:

Computer Security Institute. Sem data. "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar." Press release.

EPSTEIN, Edward Jay. Não publicado. "The Diamond Invention."

HOLWICK, Rev. David. Relato não publicado. O Sr. Rifkin teve a gentileza de reconhecer que os relatos dessa exploração diferem porque ele protegeu o seu anonimato negando-se a ser entrevistado.

CAPÍTULO 16

CIALDINI, Robert B. *Influence: Science and Practice.* Allyn and Bacon, 4.ed., 2000.

"The Science of Persuasion. Scientific American", 284:2, fev 2001.

CAPÍTULO 1 7

Algumas políticas deste capítulo baseiam-se nas idéias contidas em Wood, Charles Cresson. "Information Security Policies Made Easy". Baseline Software, 1999.

Agradecimentos

DE KEVIN MITNICK

A verdadeira amizade foi definida como uma só mente em dois corpos. Poucas pessoas na vida de alguém podem ser chamadas de verdadeiros amigos. Jack Biello foi uma pessoa dedicada e amiga que reclamou contra o tratamento ruim ao qual fui submetido nas mãos de jornalistas e dos advogados do governo. Ele foi uma voz forte do movimento Liberdade para Kevin e um escritor de talento extraordinário que elaborou artigos expondo as informações que o governo não queria que as pessoas soubessem. Jack sempre me apoiou sem medo de falar por mim e de trabalhar comigo na preparação de discursos e artigos e, em determinado ponto, ele me representou como porta-voz junto à mídia.

Assim sendo, este livro é dedicado ao meu querido amigo Jack Biello, cuja morte recente de câncer, assim que terminamos o manuscrito deste livro, me deixou uma sensação imensa de perda e tristeza.

Esta obra não teria sido possível sem o amor e apoio da minha família. Minha mãe Shelly Jaffe e minha avó Reba Vartanian deram-me amor incondicional e apoio durante toda a minha vida. Sou feliz por ter sido criado por uma mãe tão amorosa e dedicada, que também é a minha melhor amiga. A minha avó tem sido uma segunda mãe para mim, dando-me o mesmo cuidado e amor que apenas uma mãe poderia dar. Como pessoas cuidadosas e generosas, elas me ensinaram os princípios de amar o próximo e cuidar dos menos afortunados. Assim sendo, imitando o padrão de generosidade e carinho, de certa forma eu sigo os seus passos. Espero que me perdoem por tê-las colocado em segundo lugar enquanto estava escrevendo, deixando de vê-las com a desculpa do trabalho e dos prazos a cumprir. Este livro não teria sido possível sem o amor constante e apoio que guardarei sempre em meu coração.

Como queria que o meu pai. Alan Mitnick, e o meu, irmão Adam Mitnick, tivessem vivido o suficiente para abrir uma garrafa de champanhe comigo no dia em que este livro foi para as livrarias. Como vendedor e dono de empresa, meu pai me ensinou muitas coisas boas das quais nunca me esquecerei. Durante os últimos meses da vida de meu pai pude estar ao seu lado para confortá-lo da melhor maneira que pude, mas essa foi uma experiência muito dolorosa da qual ainda não me recuperei.

A minha tia Chickie Leventhal sempre terá um lugar especial em meu coração. Embora tenha se decepcionado com alguns dos erros estúpidos que cometi, ela nunca me abandonou, e sempre me ofereceu seu amor e apoio. Sacrifiquei muitas oportunidades de encontrar minha tia. meu primo Mitch Leventhal e o namorado da minha tia, Dr. Robert Berkowitz, em nossa celebração semanal do sabá.

Agradeço também muito ao namorado da minha mãe, Steven Knittle, que deu amor e apoio à minha mãe por mim.

O irmão do meu pai também merece meus agradecimentos. Pode-se dizer que herdei a minha arte da engenharia social do tio Mitchell, que sabia como manipular o mundo e as pessoas como jamais esperei entender, muito menos praticar Felizmente, ele nunca teve a minha paixão pela tecnologia dos computadores durante os anos em que usou a sua personalidade cativante para influenciar quem quisesse. Ele sempre terá o titulo de grande mestre da engenharia social

Ao escrever estes agradecimentos, percebo que tenho muitas pessoas a quem agradecer pelo seu amor, amizade e apoio. Não vou conseguir me lembrar do nome de todas as pessoas gentis e generosas que conheci nos últimos anos, basta dizer que precisaria de um computador inteiro só para armazenar todos os seus nomes. Houve várias pessoas de todas as partes do mundo que me escreveram palavras de incentivo, reconhecimento e apoio. Essas palavras significaram muito para mim, particularmente nos momentos em que mais precisei delas.

Agradeço especialmente a todos aqueles que me apoiaram, defenderam e investiram seu tempo precioso e sua energia em falar com todos que quisessem ouvir, expressando sua preocupação e repulsa ao tratamento injusto que recebi e à hipérbole criada por aqueles que buscavam lucrar com "O mito de Kevin Mitnick".

Tive a sorte de trabalhar com o autor de *best-sellers* Bill Simon. Nós trabalhamos muito bem juntos, apesar dos nossos padrões de trabalho diferentes. Bill é organizado, acorda cedo e trabalha seguindo um estilo deliberado e bem planejado. Sou grato a Bill porque ele gentilmente aceitou o meu cronograma de trabalho "tarde da noite". A minha dedicação a este projeto e as inúmeras horas de trabalho mantinham-me acordado até de manhã e isso conflitou com a programação de trabalho regular de Bill

Além de ter tido a felicidade de trabalhar com alguém que podia transformar minhas idéias em sentenças dignas de um leitor sofisticado, Bill também é (na maior parte do tempo) um homem muito paciente, que soube lidar com o meu estilo de programador focalizado nos detalhes. Sem dúvida, conseguimos. Mesmo assim, quero me desculpar com Bill nestes agradecimentos, pois sempre lamentarei ter sido a única pessoa que fez com que ele atrasasse a entrega de um trabalho pela primeira vez em sua longa carreira de autor Ele tem orgulho de ser um escritor e finalmente entendo e compartilho desse orgulho. Esperamos fazer outros livros juntos.

O prazer de estar na casa de Simon, em Rancho Santa Fé, para trabalhar, e de ser mimado pela esposa de Bill, Arynne, poderia ser considerado um dos pontos altos deste projeto. A conversa de Arynne e seus pratos serão as primeiras lembranças que terei quando pensar neste livro. Ela é uma senhora de qualidade e sabedoria, engraçada, que criou um lar aconchegante e lindo. Não vou mais conseguir beber um refrigerante dietético sem ouvir a voz dela me avisando sobre os perigos do aspartame.

Stacey Kirkland significa muito para mim. Ela dedicou muitas horas do seu tempo ajudando-me no Macintosh a criar os quadros e gráficos que deram autoridade visual às minhas idéias. Admiro suas maravilhosas qualidades. Ela é uma pessoa gentil e generosa que merece as melhores coisas da vida. Ela me incentivou como amiga dedicada e é alguém com quem me importo muito. Quero agradecer a ela pelo seu apoio e por estar presente sempre que precisei dela,

Alex Kasper, da Nexspace, não é apenas o meu melhor amigo, mas também um parceiro de negócios e colega. Juntos fizemos um programa de entrevistas de rádio pela Internet conhecido como "The Darkside of the Internet", na KFI AM 640, de Los Angeles, sob a habilidosa direção de David G. Hall. Alex deu sua valiosa assistência e consultoria para o projeto deste livro. A sua influência sempre foi positiva e útil, com uma gentileza e generosidade que quase sempre iam muito além da meia-noite. Alex e eu recentemente concluímos um filme/vídeo para ajudar as empresas a treinar seu pessoal para que aprendam a evitar os ataques da engenharia social.

Paul Dryman, da Informed Decision, é muito mais do que um amigo da família. Esse detetive particular respeitado e confiável ajudou-me a entender as tendências e os processos da condução de investigações. O conhecimento e a experiência de Paul permitiram-me abordar as questões de segurança de pessoal descritas na Parte 4 deste livro.

Como uma das minhas melhores amigas, Candi Layman ofereceu apoio e amor. Ela é uma pessoa maravilhosa e merece o melhor da vida. Durante os dias mais trágicos da minha vida, Candi sempre me deu incentivo e amizade. Sou feliz por ter conhecido um ser humano tão maravilhoso e generoso e quero agradecer por ela estar sempre a meu lado.

Certamente o meu primeiro cheque de direitos autorais vai para a minha empresa de telefonia celular, por todo o tempo que passei falando com Erin Finn. Sem dúvida, Erin é como uma alma gêmea. Somos tão parecidos que chega a assustar. Ambos amamos a tecnologia e temos os mesmos gostos para comida, música e filmes. A AT&T Wireless está perdendo dinheiro por me dar todas aquelas ligações "grátis à noite e nos finais de semana" para ligar para Erin em Chicago. Pelo menos não estou usando mais o plano Kevin Mitnick. O entusiasmo de Erin e a sua confiança em meu livro elevaram meu estado de espírito. Sou muito feliz por tê-la como amiga.

Gostaria de agradecer àquelas pessoas que representam a minha carreira profissional e que são muito dedicadas. Meus compromissos de palestras são gerenciados por Amy Gray (uma pessoa honesta e carinhosa a quem admiro e adoro). David Fugate, da Waterside Productions, é um agente literário que me defendeu várias vezes antes e depois da assinatura do contrato do livro. O advogado Gregory Vinson, de Los Angeles, que estava na minha equipe de defesa durante os longos anos da batalha contra o governo. Tenho certeza de que a sua compreensão e paciência com a minha atenção aos detalhes podem ser comparadas àquelas de Bill. Ele teve a mesma experiência trabalhando comigo nos documentos legais que escreveu em meu nome.

Tive muitas experiências com advogados, mas desejo agradecer àqueles, que durante os anos das minhas interações negativas com o sistema de justiça criminal apresentaram-se e ofereceram ajuda quando precisei desesperadamente. De palavras gentis até o envolvimento profundo com o meu caso. encontrei muitos que não se ajustam ao estereótipo do advogado egoísta. Aprendi a respeitar, admirar e apreciar a gentileza e a generosidade de espírito que recebi de tantas pessoas. Cada uma delas merece ser reconhecida com um parágrafo. Vou pelo menos mencionar o nome de todos eles, porque cada um vive no meu coração, cercado da minha gratidão: Greg Aclin, Bob Carmen, John Dusenbury, Sherman Ellison, Ornar Figueroa, Carolyn Hagin, Rob Hale, Alvin Michaelson, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Richard Sherman, Skíp Slates, Karen Smith, Richard Steingard, o honorável Robert Talcott, Barry Tarlow, John Yzurdiaga e Gregory Vinson.

Aprecio muito a oportunidade que a John Wiley & Sons me deu de escrever este livro e agradeço também à sua confiança em um autor iniciante. Quero agradecer às pessoas da Wiley relacionadas a seguir, porque tornaram este sonho possível: Ellen Gerstein. Bob Ipsen, Carol Long (meu editor e estilista de moda) e Nancy Stevenson.

Outros familiares, amigos pessoais, colegas de negócios que me aconselharam e apoiaram e que me ajudaram de várias maneiras merecem meu reconhecimento e agradecimento. São eles: J. J. Abrams, David Agger. Bob Arkow, Stephen Barnes, Dr. Robert Berkowitz, Dale Coddington. Eric Corley, Delin Cormeny, Ed Cummings, Art Davis, Michelle Delio, Sam Downing. John Draper. Paul Dryman, Nick Duva, Roy Eskapa, Alex Fielding, Lisa Flores. Brock Frank, Steve Gibson. Jerry Greenblatt, Greg Grunberg, Bill Handle. David G. Hall. Dave Harrison, Leslie Herman. Jim Hill. Dan Howard, Steve Hunt, Rez Johar, Steve Knittle, Gary Kremen. Barry Krugel, Earl Krugel. Adrian

Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, *CS* Little, Jonathan Littman, Mark Maifrett, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Munoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Kevin Poulsen, Scott Press, Linda e Art Pryor, Jennifer Reade, Israel e Rachel Rosencrantz, Mark Ross, William Royer, Irv Rubin. Ryan Russell, Neil Saavedra, Wynn Schwartu, Pete Shipley, Joh Siff, Dan Sokol, Trudy Spector, Matt Spergel, Eliza Amadea Sultan, Douglas Thomas, Roy Tucker, Bryan Turbow, Ron Wetzel, Don David Wilson, Darci Wood. Kevin Wortman, Steve Wozniak e todos os meus amigos da repetidora W6NUT (147,435 MHz) de Los Angeles.

O meu oficial da condicional, Larry Hawley, merece meus agradecimentos especiais por me dar permissão para atuar como conselheiro e consultor sobre questões relacionadas com segurança sendo autor deste livro.

Finalmente devo reconhecer os homens e mulheres da polícia. Não guardo mágoas dessas pessoas que estão apenas fazendo seu trabalho. Acredito que colocar o interesse do público à frente do próprio interesse e dedicar a sua vida ao serviço público é algo que merece respeito, e embora tenha sido arrogante às vezes, quero que todos vocês saibam que amo o meu país e farei tudo o que estiver ao meu alcance para ajudar a torná-lo um lugar mais seguro no mundo, motivo pelo qual escrevi este livro.

DE BILL SIMON

Acredito que há uma pessoa *certa* para cada um. Só que algumas pessoas não têm a sorte de encontrar ou o seu Sr. Certo ou a sua Sra. Certa. Outros têm sorte. Eu tive sorte cedo em minha vida de já ter passado alguns anos (e espero passar muitos mais) com um dos tesouros de Deus: a minha mulher Arynne. Se alguma vez me esquecer de como tenho sorte, basta prestar atenção a quantas pessoas buscam e gostam da sua companhia. Arynne, agradeço por você ter entrado na minha vida.

Enquanto escrevia este livro, contei com a ajuda de um grupo leal de amigos que me garantiram que Kevin e eu estávamos realizando o nosso objetivo de combinar os fatos e o fascínio neste livro incomum. Cada uma dessas pessoas representa o valor da verdade e da lealdade e podem ser chamadas quando eu começar o meu próximo projeto editorial. São elas: Jean-Claude Beneventi, Linda Brown, Walt Brown. Tenente Geral Don Johnson, Dorothy Ryan, Guri Stark, Chris Steep. Michael Steep e John Votaw.

Meus reconhecimentos especiais para John Lucich, Presidente da Network Security Group, que se dispôs a perder tempo com a solicitação de um amigo de um amigo, e a Gordon Garb, que gentilmente respondeu a inúmeras ligações com perguntas sobre as operações de TI.

As vezes na vida, um amigo ganha um lugar de destaque porque lhe apresentou alguém que se tornou um bom amigo seu. Na agência literária Waterside Productions, em Cardiff, Califórnia, o agente David Fugate foi responsável por conceber a idéia deste livro e por me tornar co-autor que virou amigo de Kevin. Obrigado, David! E obrigado também ao dono da Waterside, o incomparável Bill Gladstone, que conseguiu me manter ocupado com um projeto de livro após o outro: estou feliz por você estar por perto.

Em nossa casa e no meu escritório doméstico, Arynne é auxiliada por uma equipe eficiente que inclui a assistente administrativa Jessica Dudgeon e Josie Rodriguez, que cuida da casa.

Agradeço a meus pais, Marjorie e I. B. Simon, que gostaria que estivessem aqui na Terra para desfrutar do meu sucesso como escritor. E também, a minha filha Victoria. Quando estou com ela, percebo o quanto a admiro, respeito e tenho orgulho dela.

Índice

C

D

E

R

S

T

V

W

KEVIN MITNICK é consultor de segurança para corporações em vários países e co-fundador da Defensive Thinking, empresa de consultoria com sede em Los Angeles (defensivethinking.com). Ele testemunhou no Comitê do Senado para Assuntos Governamentais sobre a necessidade de legislação que garanta a segurança dos sistemas de informações do governo. Seus artigos já foram publicados na maioria das revistas e jornais especializados e ele foi convidado dos programas da Court TV, *Good Morning America* e *60 Minutes;* do *Burden of Proof* da CNN e do *Headline News,* além de ter ministrado palestras em inúmeros eventos da área. Mitnick tem um programa de rádio semanal na KFI AM 640, em Los Angeles, EUA.

WILLIAM L. SIMON é autor de sucesso de mais de uma dúzia de livros, um filme premiado e textos para a televisão.

MITNICK

A ARTE DE ENGANAR

O HACKER MAIS FAMOSO DO MUNDO REVELA COMO EVITAR O MAIS SÉRIO DE TODOS OS RISCOS DE SEGURANÇA - A NATUREZA HUMANA

Todos os firewalls e protocolos de criptografia do mundo nunca serão suficientes para deter um hacker decidido a atacar um banco de dados corporativo ou um empregado revoltado determinado a paralisar um sistema. Neste livro, Mitnick fornece cenários realistas de conspirações, falcatruas e ataques de engenharia social aos negócios - e suas conseqüências.

Convidando você a entrar na mente complexa de um hacker, este livro ilustra como até mesmo os sistemas de informações mais bem protegidos são suscetíveis a um determinado ataque realizado por um artista da trapaça passando-se por um fiscal do IR ou outro personagem aparentemente inocente. Este livro explora, de forma envolvente e agradável, o motivo pelo qual cada ataque foi tão bem-sucedido - e como ele poderia ter sido evitado.

PEARSON Education

www.makron.com.br
www.pearsonedbrasil.com

ISBN 85-346-1516-0